UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Everton Henrique Cardoso de Lira

Códigos Corretores de Erros no Ensino Médio: um estudo sobre o Código de Hamming

RECIFE
2018

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Everton Henrique Cardoso de Lira

Códigos Corretores de Erros no Ensino Médio: um estudo sobre o Código de Hamming

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Federal Rural de Pernambuco como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Profª. Drª. Márcia Pragana Dantas

RECIFE
2018

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca Central, Recife-PE, Brasil

L768c Lira, Everton Henrique Cardoso de
Códigos corretores de erros no ensino médio: Um estudo sobre o Código de Hamming / Everton Henrique Cardoso de Lira. – 2018.
116 f. : il.

Orientadora: Márcia Pragana Dantas.
Dissertação (Mestrado) – Universidade Federal Rural de Pernambuco, Mestrado Profissional em Matemática, Recife, BR-PE, 2018.
Inclui referências e apêndice(s).

1. Matemática – estudo e ensino 2. Códigos corretores de erros (Teoria da informação) 3. Didática 4. Ensino médio I. Dantas, Márcia Pragana, orient. II. Título

CDD 510

Everton Henrique Cardoso de Lira

Códigos Corretores de Erros no Ensino Médio: Um estudo sobre o Código de Hamming

Trabalho apresentado ao Programa de Mestrado Profissional em Matemática - PROFMAT do Departamento de Matemática da UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO, como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovado em ___/___/___

BANCA EXAMINADORA

Profa. Dra. Márcia Pragana Dantas (Orientadora) – PROFMAT/UFRPE

Prof. Dr. Rinaldo Vieira da Silva Junior – PROFMAT/UFAL

Prof. Dr. Marcelo Pedro dos Santos – PROFMAT/UFRPE

DECLARAÇÃO.

Eu, Everton Henrique Cardoso de Lira, CPF 068.445.174-32 declaro, para os devidos fins e efeitos, que a dissertação sob o título **Códigos Corretores de Erros no Ensino Médio: um estudo sobre o Código de Hamming**, Trabalho de Conclusão de Curso entregue como requisito parcial para obtenção do título de Mestre em Matemática, com exceção das citações diretas e indiretas claramente indicadas e referenciadas, é um trabalho original. Estou consciente que a utilização de material de terceiros incluindo uso de paráfrase sem a devida indicação das fontes será considerado plágio, e estará sujeito à processos administrativos da Universidade Federal Rural de Pernambuco e sanções legais. Declaro ainda, que respeitei todos os requisitos dos direitos de autor e isento a Pós-graduação PROFMAT/UFRPE, bem como a professora orientadora Dra. Márcia Pragana Dantas, de qualquer ônus ou responsabilidade sobre a sua autoria.

Recife, 31 de agosto de 2018.

Everton Henrique Cardoso de Lira

À minha querida, amada e saudosa mãe.

Agradecimentos

Não vou me arriscar a citar nomes nos agradecimentos, por dois motivos. O primeiro é que se assim eu fizesse, esta dissertação precisaria ter mais de mil páginas para conter os nomes de todos aqueles que me apoiaram e ajudaram no decorrer desta importante etapa da minha vida. O segundo motivo é que inevitávelmente eu iria acabar esquecendo de alguém e isso me deixaria em maus lençois! Por isso, gostaria de deixar os meus sinceros agradecimentos a todos os meus familiares (humanos e felinos), amigos, professores e colegas de classe, sem o amor, a amizade e o apoio de vocês, muito provavelmente eu não teria chegado aqui. A vocês minha gratidão!

"Tudo o que um homem imaginar, outros homens poderão fazer."
(Júlio Verne)

Resumo

Neste trabalho buscamos apresentar os Códigos Corretores de Erros e, em particular, o Código de Hamming, como um conteúdo altamente propício para ser introduzido e abordado no Ensino Médio. Com este objetivo em mente, desenvolvemos um estudo teórico de caráter bibliográfico de alguns trabalhos desenvolvidos no âmbito do PROFMAT sobre o tema, os quais apresentam propostas de aplicação destes códigos neste nível de ensino, o que constitui um processo conhecido como Transposição Didática. Em seguida, realizamos um estudo sobre o código de Hamming em sua primeira formulação encontrada em (Hamming, 1950) e em sua formulação por meio de matrizes encontrada em (Rousseau, 2015), e por fim, desenvolvemos uma sequência didática para a introdução e ensino do código de Hamming no Ensino Médio. Diante de todo este cenário, buscamos com este trabalho, contribuir no processo de introdução deste tema como um dos conteúdos a serem abordados num futuro próximo no Ensino Médio.

Palavras-chave: Códigos Corretores de Erros; Ensino Médio; Sequência Didática.

Abstract

In this work, we present the Error Correcting Codes and, in particular, the Hamming Code, as a highly suitable content to be introduced and approached in High School. With this aim in mind, we have developed a theoretical study of a bibliographic character of some works developed within the scope of the PROFMAT on the subject, which present proposals of application of these codes at this level of education, which is a process known as Didactic Transposition. Next, we conducted a study of the Hamming code in its first formulation found in (Hamming, 1950) and in its formulation by matrices found in (Rousseau, 2015), and finally, we developed a didactic sequence for the introduction and teaching of the Hamming Code in High School. In view of all this scenario, we seek with this work to contribute in the process of introducing this theme as one of the contents to be approached in the near future in High School.

Keywords: Error Correcting Codes; High School; Didactic Sequence.

Lista de ilustrações

Figura 1 – Exemplo dado por Carrocino. 31
Figura 2 – Cecília Salgado 38
Figura 3 – Mundo bipolarizado 40
Figura 4 – Claude Shannon 43
Figura 5 – Sistema de informação 45
Figura 6 – Exemplo de erro 46
Figura 7 – Doodle em homenagem a Shannon 48
Figura 8 – Computadores da época: ENIAC à esquerda e MARK1 à direita. . . . 49
Figura 9 – Richard Hamming 50
Figura 10 – Medalha Richard Hamming 51
Figura 11 – Robô e comandos pré codificação 59
Figura 12 – Cartões para obter um número natural entre 1 e 63 64
Figura 13 – Cubo unitário tridimensional. 66
Figura 14 – Cubo unitário quadridimensional. 67
Figura 15 – Cartões “Adivinhe a idade” 89
Figura 16 – Tamanho de um arquivo com uma letra. 91
Figura 17 – Tamanho de um arquivo com trecho de música. 91
Figura 18 – Tamanho de um arquivo com trecho de música. 94
Figura 19 – Matrizes geradora e de paridade 109
Figura 20 – Produto entre a matriz geradora e a transposta da matriz de paridade 110
Figura 21 – Codificação e correção 111
Figura 22 – Estrutura Básica de um computador 114
Figura 23 – O microprocessador 114
Figura 24 – Alguns dispositivos de entrada e saída. 116

Lista de tabelas

Tabela 1 – Codificação de alguns caracteres no código ASCII 44
Tabela 2 – Funcionamento do código $C(8,7)$, detector de um único erro. 55
Tabela 3 – Relação entre n, m e k. 56
Tabela 4 – Correção de um erro 60
Tabela 5 – Verificação da não ocorrência de erro 61
Tabela 6 – Distâncias mínimas e seus significados 70
Tabela 7 – Equivalência entre os digitos v_5, v_6 e v_7 e v_1, v_2 e v_4 75
Tabela 8 – Esquema para a codificação de um símbolo de $C(7,4)$ 75
Tabela 9 – Equivalência entre os digitos v_{12}, v_{13}, v_{14} e v_{15} e v_1, v_2, v_4 e v_8 82

Sumário

	Introdução	21
0.1	A escolha do tema e justificativa	22
0.2	Objetivos	25
0.3	Metodologia	25
0.4	Organização da dissertação	26
1	CÓDIGOS CORRETORES DE ERROS: PROPOSTAS PARA O ENSINO MÉDIO	27
1.1	Códigos Corretores de Erros e o empacotamento de discos	27
1.2	Explorando um contexto para o ensino de matrizes, determinantes e polinômios	29
1.2.1	Uma breve reflexão sobre a contextualização	31
1.3	Aritmética, matrizes e Códigos Corretores de Erros	32
1.4	Codificação, decodificação e Códigos Corretores de Erros com Álgebra Linear	33
1.5	64 tons de matemática	34
1.6	Uma palavra sobre a transposição didática	35
1.7	A contribuição de uma brasileira	37
2	O CÓDIGO DE HAMMING	39
2.1	Matemáticos e cientistas entram na guerra	39
2.2	Claude Shannon: o pai da teoria da informação	42
2.3	Finais de semana perdidos	48
2.4	Detectando e corrigindo erros	51
2.4.1	Códigos detectores de um único erro	54
2.4.2	Um primeiro passo na correção dos erros: códigos corretores de um único erro	56
2.4.3	Por que o Procedimento 2.16 funciona e como obtemos a Tabela 3	62
2.5	Uma interpretação geométrica	65
2.6	O código $C(7,4)$ e a famíla de códigos $C(2^k-1, 2^k-k-1)$	72
3	SEQUÊNCIA DIDÁTICA	85
3.1	1ª aula – Estrutura, funcionamento e componentes básicos de um computador	86

3.2 2ª a 4ª aulas – O sistema binário de numeração e o código ASCII 88
3.3 5ª a 8ª aulas – Explorando o Código de Hamming 95

Considerações Finais 99

REFERÊNCIAS 103

APÊNDICES 107

APÊNDICE A – O CÓDIGO $C(15, 11)$ NO EXCEL 109

APÊNDICE B – MATERIAL PARA A 1ª AULA DA SEQUÊNCIA DIDÁTICA 113
B.1 Material para a 1ª aula 113

Introdução

A Matemática, como disciplina escolar, surgiu no Brasil no início da primeira metade do século XX, por principal iniciativa e incentivo de Euclides Roxo, professor e também diretor do tradicional e prestigioso Colégio Pedro[1]II (VALENTE, 2006). Nesta mesma época, mais precisamente, no ano de 1931, ocorreu a chamada "Reforma Francisco Campos", na qual, a recém-criada disciplina passou a fazer parte dos programas de ensino das escolas brasileiras. Desde então, a melhoria na qualidade do ensino da mesma tem sido alvo de amplas discussões entre os professores, os pesquisadores da educação e os matemáticos profissionais. Os tópicos em debate abrangem temas que vão desde a maneira como devem ser estruturados e ensinados os conteúdos necessários para a formação matemática básica requerida nos ensinos fundamental e médio, até ao nível e enfoque com que devem ser abordadas as disciplinas específicas para a formação das novas gerações de professores e de matemáticos.

Atualmente, o ensino da matemática escolar é norteado por alguns documentos, dentre eles, destacamos no âmbito nacional, os Parâmetros Curriculares Nacionais - PCN que abordam os conteúdos matemáticos e a maneira como eles devem ser trabalhados tanto no Ensino Fundamental (BRASIL, 1997; BRASIL, 1998), quanto no Médio (BRASIL, 2000; BRASIL, 2002). No âmbito estadual, figuram os Parâmetros para a Educação Básica do Estado de Pernambuco - PCE-PE (PERNAMBUCO, 2012), que assim como os PCN, tratam do ensino da matemática desde os anos iniciais do Ensino Fundamental até o Ensino Médio, bem como, apontam alguns caminhos que devem ser seguidos na formação do professor de matemática (PERNAMBUCO, 2014) e no trabalho diário na sala de aula baseado em tais parâmetros (PERNAMBUCO, 2013). Há ainda, vale destacar, as mais recentes propostas de currículo apresentadas pela Sociedade Brasileira de Matemática - SBM, tanto para o Ensino Fundamental (SBM, 2015a), quanto para o Ensino Médio (SBM, 2015b) e a Licenciatura (SBM, 2015c).

Tais documentos, assim como vários outros trabalhos realizados por pesquisadores em Educação Matemática, apontam alguns caminhos que podem ser traçados pelos professores, de forma que o trabalho com a matemática na sala de aula se torne mais significativo para os alunos. Os levando assim, a um maior envolvimento com a disciplina e ao consequente rompimento com a ideia de que a matemática é difícil, complicada e que só pode ser compreendida por uns poucos "iluminados". O que tem sido uma realidade nas nossas escolas, que se faz presente desde as séries iniciais, conforme nos mostra (SILVA, 2009).

[1] Para maiores detalhes sobre a fundação e desenvolvimento deste importante Colégio ver <http://www.cp2.g12.br/images/comunicacao/memoria_historica/index.html>.

Dentre as inúmeras sugestões e propostas para melhorar o ensino da matemática no Brasil, em todos os seus níveis, destacamos o enfoque que foi dado nas Diretrizes Curriculares Nacionais para os Cursos de Matemática (BRASIL, 2001), para o papel exercido pelo professor. Neste documento, é expressa a intenção de que o egresso dos cursos de matemática – Bacharelado ou Licenciatura – seja capaz de "[...] estabelecer relações entre a Matemática e outras áreas do conhecimento" (p. 04), além de possuir "[...] conhecimento de questões contemporâneas" (idem), bem como "[...] trabalhar na interface da Matemática com outros campos do saber" (idem), dentre outras coisas.

Estas orientações nos mostram que o que se espera atualmente do profissional da matemática, em particular do professor, é a compreensão de que a Matemática não é uma disciplina isolada das outras disciplinas escolares ou dos outros campos da ciência, como também, a compreensão de que o seu desenvolvimento se dá de forma contínua e perpétua, e que a introdução de novos conteúdos da mesma nos currículos da Educação Básica, constitui uma ação não apenas possível e desejável de se fazer, mas que além disso, é necessária para o bom desenvolvimento do seu ensino, tendo em conta as novas demandas da sociedade contemporânea.

Em vistas destas considerações, nos dispomos neste trabalho a elaborar uma proposta de *sequência didática*, a qual visa a introdução e o ensino de um conceito matemático, ainda inexplorado nos currículos e livros da Educação Básica, mas que aos poucos vem sendo estudado e abordado em propostas pedagógicas para este nível de ensino, as quais sugerem o surgimento de um processo de *transposição didática* atuando sobre o conteúdo conhecido como *Códigos Detectores e Corretores de Erros*.

A seguir, apresentaremos os caminhos e os motivos que nos levaram a abordar este tema e não outro qualquer neste trabalho.

0.1 A escolha do tema e justificativa

A Guerra Fria sempre foi um período que nos chamou bastante a atenção. Num primeiro momento, a ideia de um mundo bi polarizado, onde a escolha ou o simples fato de pertencer pelo nascimento, por exemplo, a um dos lados na disputa entre Estados Unidos e União Soviética, poderia ter consequências irreparáveis para a vida dos envolvidos, nos levou a querer saber mais sobre este período ímpar na História da Humanidade.

Durante nossos primeiros estudos sobre este período, um fato que muito nos interessou, foram os desenvolvimentos tecnológicos oriundos das disputas entre estas duas nações. Viagens espaciais, armamento nuclear, veículos guiados remotamente, supercomputadores e internet são apenas alguns dos subprodutos das inúmeras pesquisas científicas empreendidas na época. Na busca pela compreensão de qual o papel da matemática neste período, pudemos perceber que grande parte do que foi produzido e desenvolvido pelos

cientistas desta época não teria sido possível, se não fosse o papel central da matemática em áreas como Engenharia, Física e Química, por exemplo.

Num segundo momento, nossa atenção voltou-se para o fato de que o desenvolvimento de importantes tecnologias digitais neste período, dentre elas a internet, só se tornaram viáveis graças ao papel desempenhado pela matemática e, em particular, por uma teoria matemática que sem a mesma, podemos afirmar sem sombra de dúvidas, o mundo digital não seria o que é hoje. Estamos nos referindo a Teoria dos Códigos Detectores e Corretores de Erros ou como comumente é chamada Teoria dos Códigos Corretores de Erros.

A Teoria dos Códigos Corretores de Erros é, grosso modo, o ramo da matemática que estuda os problemas relacionados com a eficiência e a eficácia na transmissão e recepção de informações digitais, bem como o papel do erro nesse processo. De acordo com (HEFEZ; VILLELA, 2008), um Código Corretor de Erros consiste em um procedimento desenvolvido para a transmissão de informações, no qual a introdução sistemática de informação redundante a uma informação prévia que se deseja transmitir é realizada, de forma que a informação redundante seja utilizada posteriormente na detecção e correção dos possíveis erros ocorridos neste processo de transmissão.

Vale destacar também que os Códigos Corretores de Erros são um dos grandes responsáveis pelo desenvolvimento e funcionamento de tecnologias que fazem parte do nosso dia a dia como, por exemplo, televisores, smartphones, computadores, música digital, internet e etc. Mais ainda, suas aplicações podem ser vistas nas mais diversas áreas da ciência, ver por exemplo, (GUIMARÃES, 2003) para uma aplicação na Engenharia Elétrica, (ROCHA, 2010; FARIA, 2011) para aplicações na Biologia, (AGUIAR; VIEIRA; CAVALCANTE, 2010) para uma aplicação na Computação Quântica[2] e (BOLLAUF, 2015) para uma aplicação em Criptografia.

Por esses motivos, entendemos ser relevante para os professores de matemática do Ensino Básico, a devida compreensão do que são estes códigos, para que em sua atuação nas salas de aula, os mesmos sejam capazes de abordá-los de forma clara e adequada para este nível de ensino. Além disso, entendemos que propostas como esta possuem potencial para serem geradoras de outras propostas na mesma direção, o que no futuro pode consolidar os Códigos Corretores de Erros como um tema de ensino e estudo na Educação Básica, o que dentre outras coisas, possibilitaria o despertar do interesse de jovens estudantes pela matemática e suas aplicações.

Após refletirmos sobre qual enfoque dar a Teoria dos Códigos Corretores de Erros

[2] Dentre outras coisas, a computação quântica promete revolucionar a forma como tratamos a informação e a sua transmissão. Para o leitor interessado em conhecer mais desta emergente área da computação, ver <http://www.sbmac.org.br/boletim/pdf_2004/livro_08_2004.pdf> ou o vídeo disponível em <https://www.youtube.com/watch?v=fLN1zQOPT2E>, onde o funcionamento, fundamentos matemáticos e as possiveís aplicações dos computadores quânticos são discutidos de forma introdutória.

neste trabalho, de forma que dele possam advir contribuições relevantes para o ensino da matemática a nível básico, a escolha recaiu sobre o *Código de Hamming*, desenvolvido em 1950 pelo matemático e engenheiro americano Richard Hamming (1915 - 1998). Um dos motivos para tal escolha deveu-se ao fato deste código apresentar papel de destaque no desenvolvimento inicial dos primeiros Códigos Corretores de Erros, conforme pode ser visto em (ABRANTES, 2003), bem como pelas possibilidades de abordagem do assunto, que acreditamos possíveis de serem realizadas no Ensino Médio.

Em estudos preliminares para a realização desta pesquisa, pudemos verificar que os Códigos Corretores de Erros têm sido tema de alguns trabalhos na proposta do PROFMAT. Isso nos sugere, como já dissemos anteriormente, a existência do início de uma tendência de introdução e adaptação deste assunto para a sua futura abordagem no Ensino Médio, uma vez que, o mesmo consiste em um rico tema para a contextualização de assuntos como Matrizes, Determinantes, Polinômios, Aritmética Binária, dentre outros assuntos relevantes para esse nível de ensino.

Mais precisamente, o tema "Códigos Corretores de Erros" já foi abordado por: (MIRANDA, 2013), onde o autor explora um problema mais específico da área, a saber, o chamado "empacotamento de esferas", como também apresenta uma sequência didática para o seu ensino em nível médio; (CARVALHO, 2014), como campo da matemática onde os conceitos de Matrizes, Determinantes e Polinômios são aplicados;(ALVES, 2015), como contexto para o estudo de Aritmética e Matrizes no Ensino Médio; (NICOLETTI, 2015), onde o autor destaca a relação entre o assunto e a Álgebra Linear, como também a importância de se introduzir ideias básicas do mesmo no Ensino Médio; e (DIAS, 2017), onde o autor apresenta uma aplicação dos Códigos Corretores de Erros realizada pela NASA - *National Aeronautics and Space Administration* em 1971 na Missão Mariner[3], bem como apresenta uma sequência didática para a utilização de matrizes na codificação e decodificação de mensagens. Entraremos em maiores detalhes sobre estes trabalhos mais adiante, no Capítulo 1.

Considerando o até aqui exposto, entendemos que esta dissertação se justifica por três motivos: o primeiro, foi a necessidade observada dos professores de matemática serem capazes de desenvolver propostas inovadoras para o ensino da disciplina; o segundo, foi o que entendemos ser a urgência da modernização dos conteúdos que compõem os currículos de matemática do ensino básico; e o terceiro, diz respeito ao grande potencial que acreditamos terem os Códigos Corretores de Erros, como ramo da matemática capaz de apresentar a mesma em suas inúmeras aplicações e intercessões com outras áreas do conhecimento.

[3] O programa de missões espaciais Mariner foi um dos maiores e mais importantes empreendimentos do século XX. Para o leitor interessado em conhecer mais sobre este programa ver, por exemplo, <https://www.nasa.gov/mission_pages/mariner>, onde será possível encontrar inúmeras fotos, curiosidades e histórias sobre as missões do Programa Mariner.

Particularmente, com o nosso trabalho, pretendemos aproximar os Códigos Corretores de Erros das salas de aula, através da sequência didática que propomos para o ensino do código de Hamming, o que, como será visto mais adiante, não foi tema central de nenhum dos trabalhos por nós consultados.

0.2 Objetivos

Neste trabalho temos como objetivo geral apresentar a Teoria dos Códigos Corretores de Erros como um elemento importante da matemática desenvolvida e utilizada na atualidade, bem como um tema propício para a abordagem de alguns conceitos do ensino básico, dos quais destacam-se, por exemplo, Sistema Binário de Numeração, Polinômios, Vetores, Matrizes e Determinantes.

Quanto aos objetivos específicos nos propomos a:

i) Realizar um levantamento dos trabalhos desenvolvidos na perspectiva do PROFMAT sobre Códigos Corretores de Erros, verificando assim, os avanços que já foram feitos nesta direção, bem como onde a proposta aqui desenvolvida se mostra relevante;

ii) Apresentar o código corretor de erros desenvolvido por Hamming, de forma que o mesmo possa ser compreendido e utilizado por professores e alunos do Ensino Médio;

iii) Desenvolver uma sequência didática para o ensino do Código de Hamming no Ensino Médio.

0.3 Metodologia

Tendo os objetivos acima elencados e diante das inúmeras opções metodológicas disponíveis, decidimos realizar um estudo de natureza teórica, a saber, uma pesquisa bibliográfica de textos referenciais, dentre os quais destacamos: (HAMMING, 1950), do qual apresentaremos a proposta inicial de definição e abordagem do código e (ROUSSEAU; AUBIN, 2015), no qual o Código de Hamming é abordado em sua forma atual, se utilizando de matrizes.

Vale ressaltar que (HAMMING, 1950) teve papel relevante no desenvolvimento inicial da Teoria do Códigos Corretores de Erros, pois no mesmo o Código de Hamming é pela primeira vez apresentado para a comunidade científica da época, assim como, contém importantes elementos teóricos – por exemplo, a *métrica de Hamming* – que permitiram o desenvolvimento e o aprimoramento de outros códigos que vieram depois deste.

0.4 Organização da dissertação

Esta dissertação está organizada em três capítulos. No primeiro, realizamos uma breve explanação dos trabalhos realizados no âmbito do PROFMAT sobre Códigos Corretores de Erros. No segundo, apresentamos o Código de Hamming em sua formulação original e do ponto de vista matricial, além de uma interpretação geométrica para o mesmo. Finalmente, no terceiro capítulo, desenvolvemos a sequência didática para o ensino do Código de Hamming no Ensino Médio.

1 Códigos Corretores de Erros: propostas para o Ensino Médio

Neste capítulo apresentamos e discutimos alguns trabalhos nos quais os Códigos Corretores de Erros, ou são tema de propostas de ensino ou figuram como contexto propício para o ensino de alguns conteúdos do Ensino Médio[1]. Para tanto, focaremos a nossa atenção nos trabalhos (MIRANDA, 2013; CARVALHO, 2014; ALVES, 2015; NICOLETTI, 2015; DIAS, 2017), os quais já foram citados anteriormente na introdução desta dissertação.

1.1 Códigos Corretores de Erros e o empacotamento de discos

Para iniciar, vamos considerar o trabalho em (MIRANDA, 2013), o qual está dividido em duas partes: na primeira o autor aborda conceitos básicos da transmissão de informações digitais e o papel dos códigos corretores de erros na boa transmissão destas, como também, trata de aspectos elementares do estudo do empacotamento de discos no plano, apresentando o empacotamento ótimo para este caso; na segunda parte, o autor propõe uma sequência didática dividida em três blocos de duas aulas cada, a qual visa abordar os conceitos de transmissão de informação digitais, o Código de Hamming e por fim o empacotamento de discos no plano.

Há dois pontos de vista neste trabalho que gostaríamos de destacar. O primeiro, é o matemático, pois em seus resultados o autor apresenta uma prova simples para um empacotamento ótimo, se utilizando apenas de conceitos que podem ser abordados no nível médio. O que pode se mostrar bastante útil para futuras aplicações do seu trabalho, mais precisamente, da sequência didática proposta, além disso, o autor afirma que sua abordagem para o problema é inédita (ou pelo menos diferente das abordagens tradicionais).

Em suas próprias palavras

> Na busca pelo empacotamento ótimo no plano, daremos uma definição

[1] Durante a finalização desta dissertação, entramos em contato com outros trabalhos voltados à mesma temática, os quais, não tivemos a oportunidade de incluir neste capítulo, devido ao limitado espaço de tempo que dispúnhamos para a realização do mesmo, mas que decidimos citar aqui nesta nota, pois temos a intenção de estudá-los num futuro próximo. Tais trabalhos são: Dígitos verificadores e detecção de erros (2013), de Carla Rejane Fick Pinz; Códigos Corretores de Erros: Exemplos da Matemática Aplicada em Situações do Cotidiano (2015), de Raphael Bruno Rodrigues da Silveira; Uma abordagem de dígitos verificadores e códigos corretores no Ensino Fundamental (2016), de Daniel Alves Machado; Códigos Corretores de Erros (2017), de Nicole Bertoluci Rodrigues; Códigos binários e truques de mágica (2017), de Ewerton da Silva Schroeder; e Introdução aos Métodos de Detecção de Erros em Sequências Numéricas (2017), de Sérgio Adriano Marques da Silva.

> alternativa para a densidade desse empacotamento, utilizando a triangulação de Delaunay [...]. Ressaltamos que, nas referências pesquisadas e em outras fontes que não listamos aqui, tal definição e a prova apresentada na sequência sobre a densidade ótima no plano não foram encontradas, de modo que podem ser contribuições teóricas efetivas desse trabalho. (MIRANDA, 2013, p. 24).

O segundo ponto de vista que gostaríamos de destacar é o ponto de vista da Educação Matemática, uma vez que o assunto em questão, como já citamos anteriormente, se mostra relevante e atual, e a proposta apresentada se revela totalmente de acordo com a visão exposta por Ubiratan D'Ambrosio sobre qual tipo de matemática será relevante para o ensino no futuro:

> Pode-se prever que na matemática do futuro serão importantes o que hoje se chama matemática discreta e igualmente o que se chamavam "casos patológicos", desde a não-linearidade até a teoria do caos, fractais, fuzzies, teoria dos jogos, pesquisa operacional, programação dinâmica. (D'AMBROSIO, 1996, p. 59).

Notamos que, devido a sua natureza, os Códigos Corretores de Erros podem ser inseridos nessa lista de assuntos, ou seja, podemos afirmar que as propostas de trabalho com Códigos Corretores de Erros no nível médio estão na vanguarda da introdução da matemática do século XXI no ambiente escolar. Ainda falando sobre a matemática que deve ser ensinada nas escolas no século XXI, D'Ambrosio afirma que "Justamente por representar a matemática do futuro, é muito mais interessante para o jovem. Os problemas tratados são mais interessantes, a visualização é no estilo moderno, parecido com o que se vê na TV e nos computadores". (idem). Tão relevante quanto ter a noção de qual matemática ensinar no século XXI é ter a noção de que a mesma é possível de ser ensinada na escola, pois, conforme D'Ambrosio conclui, "[...] toda essa matemática é acessível no nível primário". (idem.).

Em suma, entendemos que a proposta contida em (MIRANDA, 2013), apresenta grandes potencialidades de aplicação em sala de aula e acreditamos que tal aplicação pode render bons frutos, no que diz respeito à modernização do ensino da matemática no Ensino Médio. Entretanto, ainda não podemos afirmar quais seriam os resultados da aplicação da sequência didática desenvolvida nesta proposta, mas estamos otimistas quanto aos possíveis resultados positivos oriundos da mesma, esperamos que em estudos posteriores tenhamos a oportunidade de verificar tais expectativas.

1.2 Explorando um contexto para o ensino de matrizes, determinantes e polinômios

Continuando nossa busca por trabalhos que apresentem os Códigos Corretores de Erros como um assunto possível de ser abordado no Ensino Básico, nos deparamos com a proposta de (CARVALHO, 2014). Neste trabalho o autor tem por objetivo apresentar contextos onde matrizes, determinantes e polinômios são aplicados no cotidiano dos seus alunos, para tal, o mesmo escolhe os códigos corretores de erros como tema onde tais objetos matemáticos são utilizados, uma vez que aqueles estão intimamente relacionados com a fundamentação matemática destes.

Partindo deste pressuposto, o mesmo apresenta em seu trabalho uma formalização dos conceitos de matrizes, determinantes e polinômios, enfatizando sempre as demonstrações das propriedades elementares relacionadas aos mesmos. O autor justifica esta abordagem, se apoiando no fato de que "[...] nos livros didáticos atualmente adotados nas escolas públicas, as demonstrações estão deixando de figurar, apenas as propriedades operacionais das matrizes, determinantes e dos polinômios são apresentadas.". (CARVALHO, 2014, p. 24).

Em seguida, passa a considerar algumas estruturas algébricas elementares como, por exemplo, anéis, corpos e grupos, as quais embora não figurem nos programas nem nos livros didáticos do Ensino Básico, estão intimamente relacionadas com os conceitos de matriz, determinante e polinômio. Isso tudo é feito, para que seja apresentada uma introdução elementar aos códigos corretores de erros, na qual figuram conceitos centrais da teoria como métrica de Hamming, equivalência de códigos, códigos lineares, dentre outros. Entretanto, nosso interesse por este trabalho recai principalmente na justificativa e motivação apresentadas pelo autor para a realização do mesmo, como também nas atividades que foram propostas para abordar os conceitos de matrizes, determinantes e polinômios, no contexto do estudo dos Códigos Corretores de Erros.

Como pudemos observar nas justificativas do autor, a tônica do seu discurso está centrada na necessidade de se praticar um ensino da matemática mais próximo da realidade cotidiana dos alunos, para isso, a questão da contextualização do ensino é evocada e o autor traça considerações pertinentes sobre a mesma. Mais precisamente, destaca a necessidade de se trabalhar tanto a parte "técnica" da matemática quanto os seus aspectos práticos e as aplicações. Sobre este respeito, o mesmo afirma:

> Particularmente, reconhecemos a necessidade da resolução de exercícios do tipo "calcule", "determine" etc., porém, para um aprendizado consolidado de matemática, há necessidade de problemas que estimulem o pensar, que sirvam de ponte entre teoria e prática, que suscitem o aluno à busca por respostas tendo como referência os fenômenos da vida extraescolar. (CARVALHO, 2014, pp. 17 - 18).

Tal afirmação está de acordo com a compreensão expressa em (LIMA, 2002), pelo matemático e professor Elon Lages Lima (1929 - 2017) – o qual, durante sua carreira se mostrou bastante preocupado e engajado na busca pela melhoria do ensino de Matemática na Educação Básica – quando este trata de três aspectos do ensino da disciplina que ele considera fundamentais, a saber, *conceituação, manipulação* e *aplicações*. O mesmo concebe a relação entre estes aspectos da seguinte forma:

> Da dosagem adequada de cada uma dessas três componentes depende o equilíbrio do processo de aprendizagem, o interesse dos alunos e a capacidade que terão para empregar futuramente, não apenas as técnicas aprendidas nas aulas, mas, sobretudo o discernimento, a clareza das ideias, o hábito de pensar e agir ordenadamente, virtudes que são desenvolvidas quando o ensino respeita o balanceamento das três componentes básicas. (LIMA, 2002, p. 139).

Por outro lado, o também matemático e professor interessado na Educação Básica e formação de professores, Geraldo Ávila (1933 - 2010), em (AVILA, 2010), define três objetivos para o ensino da matemática que estão intimamente relacionados com estes aspectos. Em suas palavras:

> O ensino deve sempre enfatizar as idéias da Matemática e sua importância no desenvolvimento da própria matemática. Os diferentes tópicos da Matemática devem ser tratados de maneira a exibir sua interdependência e organicidade. O ensino da Matemática deve ser feito de maneira bem articulada com o ensino de outras ciências, sobretudo a Física. (AVILA, 2010, p. 09).

É evidente que apenas estes três aspectos e estes objetivos não são suficientes para que o ensino da matemática ocorra de forma efetiva e proveitosa para os alunos, tanto dentro como fora da sala de aula, por exemplo, aspectos sociais, psicológicos, didáticos e pedagógicos, influenciam no ensino e na aprendizagem e também devem ser considerados, pois, são tão importantes como os acima elencados. Contudo, não podemos negar que os aspectos e os objetivos apresentados pelos professores Elon e Geraldo, são de fundamental importância para que os professores de matemática de fato ensinem matemática em suas salas de aula e não apenas desenvolvam uma prática onde a matemática figura num segundo plano em relação a estes aspectos.

Ao apresentar a motivação para a realização do seu trabalho, (CARVALHO, 2014) aborda um fato interessante, a saber, que a maioria dos alunos questionados sobre onde eles aplicariam os conhecimentos sobre matrizes e determinantes na prática, afirmam que tais conhecimentos seriam "aplicados" em geometria analítica, o que mostra que a ideia de aplicação da matemática pelos alunos nessa pesquisa, se resume à aplicação da matemática nela própria, o que por si só não é de fato um problema, porém evidencia a necessidade de um trabalho com a proposta do autor, a saber, mostrar como a matemática também se faz presente no dia a dia da sociedade moderna.

1.2.1 Uma breve reflexão sobre a contextualização

A proposta de (CARVALHO, 2014) nos remete ao fato de que a questão da contextualização no ensino da matemática tem sido tema de várias discussões e críticas por parte de matemáticos e pesquisadores em educação matemática. No que diz respeito às críticas, fazemos referência ao trabalho de (CARROCINO, 2014), no qual o autor investiga o problema da contextualização em questões de matemática do Ensino Fundamental e mostra como o termo contextualização tem sido utilizado de forma equivocada, e como muitas vezes, situações onde a mesma não é possível são construídas "à força", gerando questões-problema no mínimo cômicas.

Para o leitor ter apenas uma ideia das aberrações que podem surgir nessas tentativas, reproduzimos aqui uma questão de um concurso público para Professor de Matemática do Ensino Fundamental na cidade do Rio de Janeiro retirada do trabalho deste autor, a qual diz: "Observe a "tira" abaixo.

Figura 1 – Exemplo dado por Carrocino.

Fonte: (CARROCINO, 2014, p. 36)

Ligando as extremidades dos fios dos cabelos do Cebolinha com linhas retas, desenha-se um pentágono. A soma dos ângulos internos desse polígono é de [...]" (CARROCINO, 2014, p. 36).

Tendo em vista estas considerações, nós podemos afirmar que a proposta de (CARVALHO, 2014) está de acordo com o defendido por (CARROCINO, 2014), no que diz respeito a se trabalhar questões onde a contextualização não seja forçada. Entretanto, uma crítica que acreditamos, deve ser feita ao trabalho em (CARVALHO, 2014), é devida ao fato de o mesmo afirmar que apresentaria atividades para se trabalhar com os conteúdos de matrizes, determinantes, polinômios e códigos corretores de erros, mas na realidade, o mesmo apresenta na maior parte destas ditas atividades, uma série de questões envolvendo estes assuntos, não realizando assim o proposto no inicio do trabalho, a saber, a aplicação dos códigos corretores de erros em situações práticas, como era de se esperar devido a ênfase dada pelo autor inicialmente à questão da contextualização da matemática.

Enfim, concluímos que o autor teve uma motivação boa para o trabalho, fez considerações pertinentes sobre sua problemática, mas deixou a desejar no que diz respeito a mostrar a aplicabilidade dos códigos corretores de erros na prática ou de propor atividades mais significativas relacionadas a estes, porém tais faltas não diminuem a relevância das considerações feitas no trabalho.

1.3 Aritmética, matrizes e Códigos Corretores de Erros

Seguindo uma abordagem semelhante à dos trabalhos anteriores, encontra-se o trabalho desenvolvido por (ALVES, 2015), no qual os códigos corretores de erros são o assunto de uma oficina proposta pelo autor para contextualizar o estudo de matrizes e aritmética no Ensino Médio. Esta dissertação foi organizada em seis capítulos, dos quais os cinco primeiros se ocupam em apresentar a fundamentação matemática dos códigos corretores de erros, bem como, abordar os rudimentos da teoria dos códigos lineares, dando ênfase aos códigos de Hamming e de Reed-Solomon. Não faremos considerações sobre estes capítulos, devido ao fato deles conterem o básico da Teoria dos Códigos Corretores de Erros, assunto que pode ser facilmente encontrado em qualquer das referências apresentadas pelo autor, como também nos trabalhos citados neste capítulo.

Nosso interesse recai no sexto capítulo do trabalho, onde a proposta de uma oficina envolvendo os códigos corretores de erros é apresentada, e reafirmando a relevância do tema abordado e da proposta em questão, o autor lembra ao leitor que "O professor de Matemática deve estar ciente de sua responsabilidade em estar sempre atento aos avanços da Matemática, principalmente àqueles que estão presentes diretamente no cotidiano de seus alunos." (ALVES, 2015, p. 51) e conclui que tal postura exige do professor a capacidade de relacionar a matemática estudada na escola com a sua utilização fora dela, e que nesta tarefa "A oficina surge como metodologia apropriada a desenvolver essa relação entre teoria e prática, dando um aspecto mais concreto a diversos conteúdos." (idem).

A oficina foi organizada em dez aulas de 50 minutos, podendo em algumas aulas o tempo ser ampliado ou reduzido, conforme verificada a necessidade pelo professor. Cada aula é estruturada nos seguintes tópicos: tema, tempo estimado, conteúdo, objetivos, estratégias de ensino, recursos didáticos e avaliação. O tema diz respeito ao conceito da Teoria dos Códigos Corretores de Erros que vai ser abordado na aula; o tempo estimado como já dissemos acima é a duração de cada aula, que vale lembrar, não é rígido e pode variar conforme a resposta dos alunos às atividades; o tópico conteúdo diz respeito aos conteúdos matemáticos envolvidos no tema da aula como, por exemplo, matrizes e sistemas de numeração; em objetivos o autor coloca o que o professor procura ensinar ou verificar em seus alunos através da atividade; em estratégias de ensino são abordadas as possíveis ações

do professor na tentativa de alcançar os objetivos propostos com a aula; recursos didáticos dizem respeito a todo o material que o professor necessitará em cada aula para aplicar a atividade, tais recursos vão desde o quadro e lápis até o uso da internet; e por fim, com o tópico avaliação, procura-se verificar a participação dos alunos e o seu desenvolvimento individual com respeito a aprendizagem do conteúdo em questão.

Finalmente, apresentada esta proposta de oficina, somos levados a concordar com as palavras do autor quando este finaliza seu trabalho afirmando que

> O motivador deste trabalho é a situação do ensino de Matemática no país. Apesar da constante cobrança em alterar a metodologia de ensino, majoritariamente expositiva, não é fornecido meios que permitam aos professores conhecerem e utilizarem de outras metodologias. A oficina exposta neste trabalho possui uma ideia. Mesmo que diversos professores conheçam o funcionamento de uma oficina, existem aqueles que não compreendem todo o potencial em se trabalhar com essa metodologia. (ALVES, 2015, p. 65).

De fato, além de ser uma ferramenta altamente dinâmica e estimulante, a oficina elaborada neste trabalho mostra possibilidades tanto para se introduzir um novo tópico da matemática presente na atualidade, quanto para trabalhar "velhos conhecidos" de professores e alunos nas salas de aula como é o caso, por exemplo, das matrizes.

1.4 Codificação, decodificação e Códigos Corretores de Erros com Álgebra Linear

Mais um trabalho por nós verificado foi o desenvolvido por (NICOLETTI, 2015), o qual destaca a importância da Álgebra Linear como teoria matemática fundamental na construção da Teoria dos Códigos, em particular dos Códigos Corretores de Erros. A dissertação deste autor está organizada em sete capítulos, dos quais além do primeiro e do último que consistem da introdução e considerações finais do trabalho, estão os capítulos 2, 3, 4 e 5 que apresentam os conceitos básicos da Teoria da Informação e da Teoria dos Códigos Corretores de Erros e o capítulo 6 que se presta a apresentação de três sequências didáticas.

Sobre o capítulo 6, vale destacar que as sequências didáticas apresentadas não trataram especificamente de um dado tipo de código corretor de erros, mas sim do processo de codificação e decodificação de mensagens, se utilizando dos conceitos de matriz e matriz inversa. Embora os conceitos de transmissão de mensagens através da codificação e decodificação façam parte da Teoria dos Códigos Corretores de Erros, questões essenciais da Teoria como, por exemplo, *detecção e correção de erros* não foram abordadas nas sequências didática, o que é uma pena, visto que dentre os autores por nós consultados,

este foi o que mais deu ênfase à experiência do aluno, aplicando suas sequências em sua turma e verificado os resultados *in locus*.

Em suma, embora (NICOLETTI, 2015) aborde os Códigos Corretores de Erros em seu trabalho, pudemos verificar que as implicações pedagógicas do mesmo não incluem uma abordagem efetiva destes na sala de aula, entretanto, entendemos ser relevante a citação do mesmo aqui, visto que isto reforça ainda mais, a ideia de que a Teoria dos Códigos Corretores de Erros se apresenta como uma forte candidata a fornecer conteúdos relevantes de serem ensinados nesse nível de ensino.

1.5 64 tons de matemática

Para encerrarmos nossas considerações sobre trabalhos anteriores no âmbito do PROFMAT, vale destacar aqui o trabalho desenvolvido recentemente por (DIAS, 2017), no qual o autor estuda o código corretor de erros utilizado na missão espacial Mariner 9, a qual foi responsável pelo envio à Terra de mais de 7000 fotos da superfície de Marte em 1971, o que possibilitou, dentre outras coisas, um considerável avanço nos estudos da geografia da superfície marciana.

O autor chama a atenção em seu trabalho para o papel exercido pelos Códigos Corretores de Erros na missão Mariner, bem como, apresenta elementos básicos da Teoria dos Códigos Corretores de Erros como, por exemplo, *distância de Hamming, distância mínima, peso, capacidade de correção e parâmetros de um código*. Em seguida, apresenta os códigos de Reed-Muller de 1ª ordem, como também os processos de codificação e decodificação de mensagens com base nestes códigos.

O ponto alto deste trabalho é quando o autor nos mostra como o código utilizado na Mariner 9 funciona, mais precisamente, como cada foto (em preto e branco) enviada pela nave foi decomposta em seus múltiplos tons de cinza (neste caso, 64), de forma que cada tom de cinza fosse representado por uma sequência binária de 6 dígitos, onde o branco foi representado por 000000 e o preto por 111111. A partir daí, cada tom de cinza foi codificado em outra sequência binária (agora com 32 dígitos, 6 de informação e 26 de verificação) e enviada pela nave à Terra. Quando a sequência fosse recebida, o procedimento do código de Reed- Muller forneceria a decodificação da sequência original, com a consequente correção dos erros (neste caso, até 7 erros), caso fossem verificados. Nas palavras do próprio autor

> O código utilizado pela Mariner 9 possui 64 palavras: isto consiste em atribuir, pela codificação da fonte, a 64 tons de cinza pré-estabelecidos, sequências binárias de comprimento 6, sendo o branco denotado por 000000 e o preto por 111111. Já pela codificação de canal [...] essas sequências binárias de comprimento 6 são transformadas em sequências binárias de comprimento 32, as quais representam os mesmos 64 tons

> de cinza, sendo o branco denotado por $\underbrace{000\ldots0}_{32}$ e o preto por $\underbrace{111\ldots1}_{32}$. (DIAS, 2017, p. 17).

Para encerrar seu trabalho o autor apresenta uma proposta de atividade para ser aplicada em sala de aula com alunos do 2º ano do ensino médio, mais precisamente, uma proposta de utilização de matrizes na codificação e decodificação de mensagens binárias. Entretanto, pudemos observar que a proposta sugerida pode demandar dos alunos uma compreensão de multiplicação de matrizes e resolução de sistemas lineares que está além do exigido neste nível de ensino, uma vez que, a realização das atividades propostas encontram-se matrizes de ordem elevada – na ocasião o autor trabalha com uma matriz 5×9. E como bem observou (ALVES, 2015), as operações com matrizes e sistemas lineares de ordem maior que 3 ainda geram algumas dificuldades para os alunos, porém entendemos que nada impede que, em situações ideais, tal sequência possa ser aplicada com sucesso.

1.6 Uma palavra sobre a transposição didática

Do exposto até aqui, podemos perceber que os Códigos Corretores de Erros estão passando por uma espécie de processo ou tratamento com vistas a torná-lo um assunto ensinável em nível médio. Mais ainda, percebemos que os Códigos Corretores de Erros também têm sido abordados em algumas obras de divulgação matemática recentes, ver (STEWART, 2013) e (MILIES, 2008), para uma abordagem mais intuitiva e informal como também, (SHINE, 2009) e (SÁ; ROCHA, 2012) e o já citado (ROUSSEAU; AUBIN, 2015), para abordagens mais técnicas, porém elementares.

Quando observamos a dinâmica presente na evolução dos Códigos Corretores de Erros, que vai desde o seu desenvolvimento inicial na segunda metade do século XX, como uma ferramenta específica para uso militar e das Engenharias, até o momento presente, em que os mesmos são tema de trabalhos acadêmicos, que visam o seu ensino escolar ou a sua consideração como contexto fértil para a aplicação de conteúdos específicos da matemática escolar, podemos notar que estes estão passando pelo processo conhecido como transposição didática, definido em (CHEVALLARD, 1989, p. 09) como segue:

> Corpos de conhecimento, com poucas exceções, não são concebidos para serem ensinados, mas para serem *usados*. Ensinar um corpo de conhecimento é, portanto, uma tarefa altamente artificial. A transição do conhecimento considerado como uma ferramenta a ser posto em prática, para o conhecimento como algo a ser ensinado e aprendido, é precisamente o que eu tenho chamado de *transposição didática* do conhecimento.

No caso dos Códigos Corretores de Erros, podemos ver claramente que, como *corpo de conhecimento* – por corpo de conhecimento (CHEVALLARD, 1989, p. 11) entende ser "[...] um todo organizado e mais ou menos integrado" – os mesmos foram inicialmente

desenvolvidos para serem apenas utilizados, não havia uma ideia inicial relacionada com o seu ensino. Contudo, conforme estes foram se mostrando altamente necessários no funcionamento de computadores e tecnologias digitais afim, pesquisadores e professores envolvidos com os mesmos passaram a desenvolver materias cujo objetivo era o de ensinar tal conteúdo para as novas gerações de estudantes e pesquisadores da área[2].

Isso vem reforçar a noção defendida em (CHEVALLARD, 1989) de que o conhecimento que é ensinado na escola (ou mesmo na graduação) não é exatamente o mesmo desenvolvido pelos pesquisadores das respectivas áreas do conhecimento na academia, mas sim, uma derivação destes, os quais passam por uma série de recortes, adaptações, organizações e reorganizações (transposição didática) com o fim de se tornarem ensináveis. Além disso, seja qual for o conhecimento que se pretenda ensinar na escola, é fato que "uma mudança profunda ocorre sempre que o conhecimento adentra o sistema de ensino.". (CHEVALLARD, 1989, p. 12).

Ainda sobre o processo de transposição didática, é posto que o mesmo ocorre, em geral, em dois grandes momentos, por assim dizer. O primeiro, chamado de transposição didática externa, que "[...] toma como referência as transformações, inclusões e exclusões sofridas pelos objetos de conhecimento, desde o momento de sua produção até o momento em que eles chegam à porta das escolas." (PERNAMBUCO, 2012, p. 24), e o segundo, chamado de transposição didática interna, que

> [...] se apresenta, por sua própria natureza, no interior da escola, e, mais particularmente, em cada sala de aula. É o momento em que cada professor vai transformar os conhecimentos que lhe foram designados para ensinar em objetos de conhecimento efetivamente ensinados. (ibid. p. 25)

Em suma, na *transposição didática externa*, o saber científico é transformado, tendo em vistas as demandas apresentadas pela sociedade e pela escola de tornar tal saber em saber ensinável e na *transposição didática interna*, temos o trabalho do professor como o responsável por realizar recortes, adaptações e modificações com o fim de efetivar a aprendizagem do agora ensinável, saber escolar.

Tendo em vista o acima exposto, gostaríamos de reforçar a importância dos trabalhos mencionados neste capítulo, bem como deste trabalho, no processo de transposição didática que os códigos corretores de erros vêm passando na última década e esperamos que as contribuições aqui dadas sejam úteis para o avanço e melhoria do ensino da matemática em nível básico. Porém antes de encerrarmos este capítulo, gostaríamos de deixar registrado

[2] Alguns dos primeiros livros voltados ao ensino desta "nova matemática" são por exemplo, The mathematical theory of comunication (1963), de Claude Shannon e Warren Weaver e Error- correcting Codes (1961), de W. Wesley Peterson e E. J. Weldon, Jr., ambos contendo resultados atualizados das últimas pesquisas da área, porém tendo como objetivo maior apresentar, divulgar e ensinar estes resultados.

aqui o avanço que tem sido feito na pesquisa sobre Códigos Corretores de Erros no Brasil, em partícular, gostaríamos de discorrer brevemente sobre a contribuição da pesquisadora da Universidade Federal do Rio de Janeiro - UFRJ, Cecília Salgado, a qual recentemente foi premiada por seu trabalho com Códigos Corretores de Erros.

1.7 A contribuição de uma brasileira

Nesta seção não consideraremos as novas aplicações, os novos desenvolvimentos teóricos ou mesmo os trabalhos voltados a divulgação dos Códigos Corretores de Erros para um público mais especializado como, por exemplo, minicursos ou palestras sobre o tema em eventos, simpósios ou encontros de matemáticos, o que diga-se de passagem, tem sido feito com certa regularidade. Em vez disso, daremos destaque aqui à pesquisadora brasileira Cecília Salgado Guimarães Silva, que em 2015 venceu a 10ª edição do prêmio **L'Oréal-UNESCO-Academia Brasileira de Ciências "Para Mulheres na Ciência"**, o qual, desde 2006 vem contemplando pesquisadoras que se destacaram no trabalho em Ciências e que tem como objetivo recompensar e dar visibilidade internacional para tais pesquisadoras, contribuindo assim para o avanço da presença feminina nas ciências.

Um rápido olhar na carreira[3] desta pesquisadora nos mostra que em 2002, Cecília Salgado graduou-se em Matemática pela Universidade Federal do Rio de Janeiro – UFRJ, obteve o grau de Mestre em Matemática pelo Instituto de Matemática Pura e Aplicada – IMPA em 2004 e em 2009 foi titulada Doutora em Matemática pela Université Paris Diderot, PARIS 7, na França. No período de 2009 a 2011 realizou estudos de pós-doutorado no Hausdorff Institute - Bonn, na Alemanha, na Universiteit Leiden, na Holanda e no Max Planck Institute fur Mathematik, também na Alemanha. Atualmente, é professora Adjunta na Universidade Federal do Rio de Janeiro, atuando no Instituto de Matemática da instituição, ministrando aulas, organizando projetos e orientando alunos e novos pesquisadores tanto em cursos de graduação como de pós-graduação. O que, dentre outras coisa, a coloca no cerne dos desenvolvimentos de pesquisa e ensino de matemática[4] de alto nível em nosso país.

No vídeo promocional publicado pelo site do prêmio,[5] Cecília Salgado nos dá uma breve explicação de qual o papel dos Códigos Corretores de Erros e da matemática na atualidade. Sobre os códigos ela afirma: *"Os códigos, eles estão por todos os lugares, TV, Internet, DVD's, sua conta de banco, ou seja, eles são realmente aplicáveis a quase tudo que você pode imaginar"*. E sobre a matemática conclui *"[...] Eu acho que, do ponto de vista de várias inovações que a gente tem vivido ultimamente, você não tem mais fronteira*

[3] Para maiores detalhes ver <http://lattes.cnpq.br/6394520126732800>

[4] Para os interessados, um vídeo onde Cecília Salgado divulga parte do seu trabalho pode ser visto em <https://www.youtube.com/watch?v=hAaxsYKZHuo>

[5] <http://www.paramulheresnaciencia.com.br/cecilia-salgado-vencedora-do-premio-para-mulheres-na-ciencia-2015/>

Figura 2 – Cecília Salgado

Fonte: Google Images

do que é matemática, as vezes, você encontra ela nos lugares mais inesperados [...].". Sobre o seu papel no trabalho com os códigos ela coloca:

> Meu trabalho é sobre Códigos Corretores de Erros em superfícies algébricas. [...] E assim, surgiram alguns exemplos de códigos muito bons usando superfícies algébricas, então a ideia é realmente a gente poder unificar todos esses exemplos dentro de uma teoria que seja mais uniforme.

Em suma, tanto os trabalhos anteriormente considerados, quanto o trabalho e o depoimento desta pesquisadora nos mostram como os Códigos Corretores de Erros são um tema atual em matemática, em pleno desenvolvimento, cuja pesquisa ainda tem muito a nos revelar sobre a sua utilidade no futuro. Por este motivo, entendemos que o professor de matemática da Educação Básica deve ter a oportunidade tanto de conhecer os códigos em sua natureza teórica e prática, bem como nas propostas de abordagem em sala de aula que tem sido feitas ultimamente. Daí a importância de trabalhos como este que está a se realizar.

Feitas estas considerações, alcançamos o primeiro dos nossos objetivos propostos. Passamos agora ao próximo capítulo, onde desenvolvemos a teoria do Código de Hamming com vistas a sua aplicação no Ensino Médio.

2 O código de Hamming

Neste capítulo, apresentamos duas formulações para o código de Hamming. A primeira (na Seção 2.4), baseada no trabalho original do autor (HAMMING, 1950), é desenvolvida a partir de procedimentos para codificação, decodificação e correção de um erro, os quais, por sua vez, estão fundamentados na relação existente entre a escrita de um número em sua forma decimal e sua forma binária. A segunda formulação (na Seção 2.6), baseada em (ROUSSEAU; AUBIN, 2015), se utiliza do conceito de matriz e da multiplicação destas para codificar, decodificar e corrigir um erro em um símbolo de código. Além disso, na Seção 2.5 apresentamos os códigos corretores de erros sob um ponto de vista geométrico, abordando alguns conceitos elementares para isso como, por exemplo, a métrica de Hamming.

Toda esta discussão é precedida por uma breve explanação do contexto político e do período histórico, nos quais Hamming e os primeiros engenheiros e matemáticos a trabalharem com Códigos Corretores de Erros viveram.

2.1 Matemáticos e cientistas entram na guerra

Com o término da Segunda Guerra Mundial, grandes nações como Inglaterra, Alemanha e França perderam muito da influência que tinham sobre a política e a economia mundial anterior à guerra, passando assim para Estados Unidos e União Soviética o "bastão" na corrida pelo controle político e econômico mundial. Sobre essa relevância conquistada, por exemplo, pela União Soviética pós Segunda Guerra, o historiador Yuval Harari afirmou "A União Soviética entrou na guerra como um isolado pária comunista. Dela emergiu como uma das duas superpotências globais e líder de um bloco internacional em expansão.". (HARARI, 2016, p. 268).

Fato marcante no período pós segunda guerra, considerado um dos mais tensos e críticos da história moderna, foi o incansável confronto entre Estados Unidos e União Soviética, o qual ficou marcado tanto pelas inúmeras disputas travadas por estas potências, quanto pelos incríveis avanços tecnológicos alcançados pelas mesmas. Tal período ficou conhecido como Guerra Fria, devido ao fato de que os confrontos entre estes gigantes globais estarem mais relacionados aos campos político, cultural e ideológico do que aos confrontos armados em si.

Embora nessa época tenham ocorrido vários confrontos armados envolvendo os exércitos de nações apoiadas pelos Estados Unidos e pela União Soviética como, por exemplo, nas guerras da Coréia (1950 - 1953) e do Vietnã (1955 - 1975), definitivamente

Figura 3 – Mundo bipolarizado

Fonte: Google Images

os dois oponentes nunca declararam formalmente guerra um ao outro, nem tiveram seus exércitos se confrontando pessoalmente. De uma forma mais precisa e resumida, podemos identificar a Guerra Fria como a época onde, verificou-se "[...] um mundo bipolarizado, que opõe: de um lado, os Estados Unidos e de outro, a União Soviética; o primeiro defendendo o capitalismo, o segundo um modelo de socialismo estatizante [...]". (VIEIRA; MUNHOZ, 2008, p. 20).

Vale salientar que uma das características mais marcantes dos Estados Unidos em relação à Guerra Fria foi o "[...] massivo investimento público em Pesquisa e Desenvolvimento (P&D), sendo o Governo Federal o principal articulador da estratégia de supremacia em C&T&D.". (SILVA, 2014, p. 03).[1]. Com tal estratégia em pauta, os Estados Unidos criaram agências específicas para este propósito como, por exemplo, a DARPA - *Defense Advanced Research Projects Agency*, a qual "[...] teve a função de desenvolver estudos novos, revolucionários e de risco, como foram os casos das pesquisas e desenvolvimentos tecnológicos da Internet; dos Veículos não tripulados; das armas e munições de precisão guiada; e da tecnologia Stealth [...]". (idem).

Neste contexto de um grande desenvolvimento tecnológico podemos destacar, por exemplo, o assombroso avanço na ciência dos foguetes mencionado por (BLAINEY, 2011) em seu livro "*Uma breve história do século XX*". Neste livro, o autor mostra como, no pequeno espaço de aproximadamente 30 anos, esta ciência evoluiu da simples construção de pequenos projéteis não tripulados – que alcançavam apenas algumas centenas de metros de altura antes de explodirem ou retornarem ao solo – para o desenvolvimento de perigosos mísseis altamente destrutivos e de sofisticadas naves espaciais tripuladas, capazes de sair

[1] C&T&D - Ciência&Tecnologia&Defesa.

da superfície terrestre, pousar em um corpo celeste, como a Lua, e retornar à Terra com todos os seus tripulantes em segurança.

Vale salientar ainda que algumas destas tecnologias se converteram em benefícios práticos para a sociedade pós Guerra Fria. A esse respeito, (KENSKI, 2011, p. 16) afirma:

> Muitos equipamentos, serviços e processos foram descobertos durante a tensão que existiu entre Estados Unidos e União Soviética pela ameaça, de ambos os lados, de ações bélicas, sobretudo com o uso da bomba atômica. A corrida espacial, resultante do avanço científico proporcionado por essa tensão, trouxe inúmeras inovações: o isopor, o forno de micro-ondas, o relógio digital e o computador.

Complementando suas considerações sobre esse assunto, Kenski traz a fala do jornalista Fábio Reynol, o qual o aborda nos seguintes termos:

> [...] os aparelhos automáticos para medir pressão arterial encontrados nas portas das farmácias são a evolução de equipamentos desenvolvidos para astronautas, que precisavam de sistemas práticos para avaliar a saúde no espaço. A válvula de um novo tipo de coração artificial foi inspirada em uma bomba de combustível de foguetes. Marca-passos são monitorados graças à mesma tecnologia utilizada em satélites. E até a Fórmula 1, famosa por ser uma grande fonte de tecnologia, copiou dos trajes espaciais os macacões antichamas de seus pilotos. Detectores de fumaça e de vazamento de gás, tão comuns em construções hoje em dia, vieram de pesquisas de similares que equipam veículos espaciais. Também é graças ao espaço que os ortodontistas contam hoje com o Nitinol, uma liga que, por ser maleável e resistente, é muito empregada na fabricação de satélites e que agora também compõe os "araminhos" de muitos aparelhos ortodônticos. E até a asa-delta, quem diria, não foi invenção de esportistas, mas de Francis Rogallo, projetista da Nasa, que desenvolveu o aparato para guiar espaçonaves depois da reentrada na atmosfera. (KENSKI, 2011, pp. 16 - 17).

Tais considerações nos mostram e reafirmam como as disputas entre estes dois gigantes foram de inigualável importância para o desenvolvimento da ciência – em particular Ocidental – e de novas tecnologias, muitas das quais, hoje são amplamente utilizadas pela sociedade. Também podemos ver que o contexto no qual os primeiros Códigos Corretores de Erros foram desenvolvidos era o mais propício para tal, visto que além da demanda para o desenvolvimento dos mesmos, havia um constante, volumoso e intenso investimento e apoio financeiro por parte do Governo - em particular o americano - o qual possibilitou aos matemáticos e cientistas da época contribuírem para a vitória de seu país[2] na guerra

[2] Cabe aqui uma resalva para o sentido da expressão *vitória de seu país*. Nesta época, uma expressiva quantidade de cientistas e matemáticos vivendo e trabalhando tanto nos Estados Unidos, quanto na União Soviética eram migrantes, refugiados ou exilados políticos oriundos de países que na Segunda Guerra Mundial tinham sido dominados pela Alemanha Nazista. Outra grande fonte de recrutamento de cientistas e matemáticos ocorreu após o término da Segunda Guerra, através das operações *paperclip* e *osoaviakhim*, dos americanos e soviéticos, respectivamente. Assim, ao nos referirmos à vitória de seu país, estamos nos referindo não somente ao país de origem, mas também ao país onde tais cientistas e matemáticos viviam e trabalhavam após serem recrutados. Um vídeo explanatório sobre estas operações pode ser acessado no link: <https://www.youtube.com/watch?v=_Q3f21Kk6kI>

através de suas melhores armas, a saber, sua inteligência, conhecimento e inventividade.

2.2 Claude Shannon: o pai da teoria da informação

Foi justamente nesse clima de tensão, novidades e competição expostos anteriormente que os rudimentos da Teoria da Informação e da Teoria dos Códigos Detectores e Corretores de Erros foram desenvolvidos pelos maiores matemáticos e engenheiros que viviam em solo americano na época . Grande parte do trabalho inicial foi realizado por homens como Claude Shannon (1916 – 2001), Richard Hamming (1915 – 1998), Irving Reed (1923 – 2012), Gustave Solomon (1930 – 1996), Marcel Golay[3] (1902 – 1989), dentre outros.

No que diz respeito à Teoria da Informação, muito do que foi inicialmente desenvolvido deveu-se ao trabalho de Shannon, o qual, ao abordar inicialmente o problema da comunicação:

> [· · ·] mergulhou no trabalho [· · ·] se concentrando nos fundamentos matemáticos da comunicação secreta – criptografia – e criando uma prova matemática para demonstrar que o chamado Sistema X, uma linha telefônica direta entre Winston Churchill e o presidente Roosevelt era seguro. (GLEICK, 2013, pp. 12 - 13).

Isso reflete, desde cedo, o seu interesse nas questões relacionadas com a comunicação, interesse este que estava, como vimos anteriormente, subsidiado pelas iniciativas do governo americano que, no início da Guerra Fria, já percebia a importância e o papel exercido pela comunicação na guerra, uma vez que a transmissão correta e eficiente de informações poderia, neste contexto, determinar, em certa medida, quem sairia vencedor no final[4].

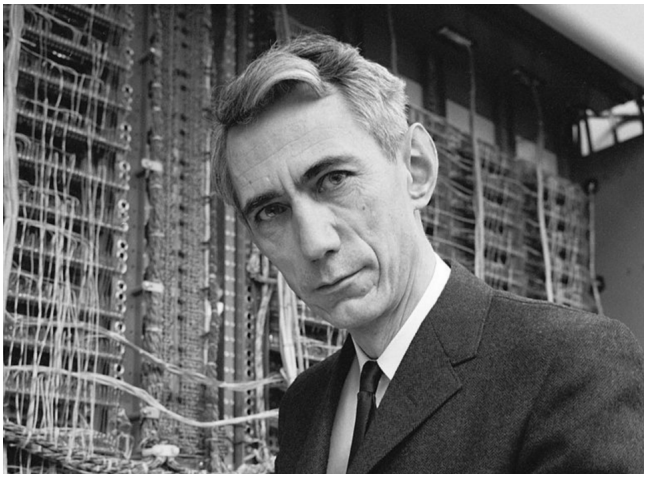
O trabalho mais importante de Shannon, intitulado *A Mathematical Theory of Communication* (SHANNON, 1948) - publicado em 1948 no *The Bell System Technical Journal*[5], um importante periódico voltado aos aspectos científicos e técnicos da comunicação na época - rendeu a ele o título de "Pai da Teoria da Informação" e foi o responsável

[3] Vale mencionar aqui que Golay foi o primeiro a desenvolver um código corretor de erros, seu código foi publicado num breve artigo intitulado *Notes on Digital Coding*, o qual, embora contenha apenas uma página não deixa de ser relevante para o desenvolvimento de códigos posteriores. Para o leitor interessado, a leitura deste artigo pode ser feita acessando: <https://www.lama.univ-savoie.fr/~hyvernat/Enseignement/1617/info528/TP-Golay/golay_paper.pdf>.

[4] Um bom exemplo do que estamos nos referindo pode ser observado na experiência vivida pelos Britânicos, na interceptação e decifração das mensagens enviadas pelos Alemães através da máquina "Enigma" durante a Segunda Guerra Mundial. Para mais detalhes sobre como os Britânicos foram capazes de quebrar o código da Enigma e, a partir daí, se utilizar de valiosas informações transmitidas pelos Alemães ver (SING, 1997, pp. 147 - 157). Também vale destacar aqui o filme "O jogo da imitação", de 2015, que embora não totalmente fiel aos fatos históricos, apresenta de forma empolgante e apaixonante o trabalho pioneiro dos matemáticos envolvidos na árdua tarefa de quebrar o código da Enigma.

[5] Para maiores detalhes sobre este periódico ver: <https://en.wikipedia.org/wiki/Bell_System_Technical_Journal>

Figura 4 – Claude Shannon



Fonte: Google Images

pelo estabelecimento das bases teóricas que possibilitaram, dentre outras coisas, o desenvolvimento dos Códigos Corretores de Erros por figuras como Richard Hamming e os seus companheiros.

Neste seu trabalho Shannon estudou o problema fundamental da comunicação, que segundo ele "[...] é o de reproduzir em um ponto exatamente ou aproximadamente uma mensagem selecionada em outro ponto." (SHANNON, 1948, p. 01, tradução nossa). Para isso, ele definiu inicialmente uma *unidade de medida de informação*, que chamou de *bit* (abreviação de binary digits) e um *sistema de comunicação*, o qual é formado basicamente por cinco componentes, a saber: *uma fonte de informação*, que produz a mensagem a ser transmitida; *um transmissor*, que atua sobre a mensagem produzindo um sinal passível de ser transmitido; *um canal*, que consiste basicamente do meio utilizado para transmitir o sinal do transmissor até o receptor; *um receptor*, que decodifica o sinal recebido na mensagem enviada pelo transmissor; e *um destino*, que é a pessoa ou equipamento que recebe a mensagem enviada[6].

Tais conceitos foram amplamente utilizados e aproveitados para o estabelecimento da Teoria dos Códigos Detectores e Corretores de Erros por dois motivos. O primeiro, foi o fato de o bit se tornar uma unidade de medida para a informação, possibilitando assim, o tratamento científico da informação, o que já ocorria há séculos com outras grandezas como, por exemplo, as físicas. O segundo, foi a sistematização do processo de comunicação, o que, dentre outras coisas, possibilitou uma ampla compreensão de como o erro interfere neste, como também levou Shannon a mostrar que "[...] existe um limite fundamental de quanta informação um canal de comunicação pode transportar." (STEWART, 2013, p.

[6] Para maiores detalhes sobre os componentes de um sistema de informação, ver (GLEICK, 2013, p. 231) e (SHANNON, 1948, p. 02)

327). A partir desta constatação os cientistas da área buscaram desenvolver métodos e códigos eficientes para a transmissão de informações em suas mais diversas formas, sem contudo se preocuparem com a quantidade máxima de informação que um canal poderia transportar visto que este problema já estava resolvido.

Tabela 1 – Codificação de alguns caracteres no código ASCII

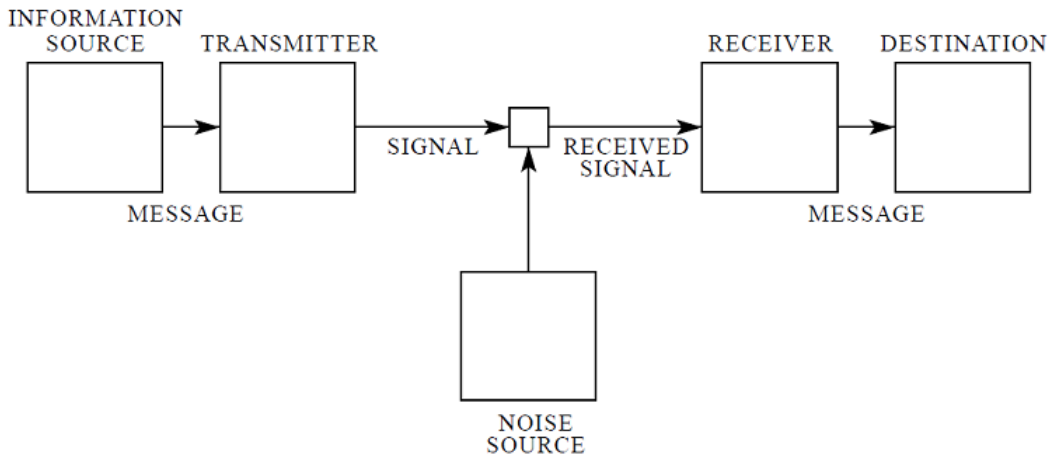
Caracter	Código ASCII	Caracter	Código ASCII
Espaço	0100 0000	M	1010 1101
.	0100 1110	N	1010 1110
(	0100 1000	O	1010 1111
+	0100 1011	P	1011 0000
$	0100 0100	Q	1011 0001
*	0100 1010	R	1011 0010
)	0100 1001	S	1011 0011
-	0100 1101	T	1011 0100
/	0100 1111	U	1011 0101
'	0100 1100	V	1011 0111
,	0100 0111	W	1011 0111
=	0101 1101	X	1011 1000
A	1001 0001	Y	1011 1001
B	1010 0010	Z	1011 1010
C	1010 0011	0	0101 0000
D	1010 0100	1	0101 0001
E	1010 0101	2	0101 0010
F	1010 0110	3	0101 0011
G	1010 0111	4	0101 0100
H	1010 1000	5	0101 0101
I	1010 1001	6	0101 0110
J	1010 1010	7	0101 0111
K	1010 1011	8	0101 1000
L	1010 1100	9	0101 1001

Fonte: O autor

Um bit de informação consiste basicamente de uma sequência contendo apenas um dos dígitos 0 ou 1. De forma análoga, se define um *byte* como uma sequência composta de oito bits. De posse destas ideias, na década de 1960 os engenheiros e cientistas da computação norte-americanos criaram o chamado código ASCII - *American Standard Code for Information Interchange*, com o qual foi possível, além de associar as letras, os algarismos e alguns sinais gramaticais a um byte (sequência de 8 bits), determinar o tamanho de uma mensagem qualquer pela contagem de seus bytes, de forma, que hoje é comum observarmos arquivos com 1Mb, 2,34Gb ou 203Kb de tamanho, por exemplo.

Sobre o papel do erro no processo de comunicação, o diagrama da Figura 5 nos mostra que, entre a transmissão e a recepção de uma dada mensagem, ocorre um ruído, ou seja, uma interferência que eventualmente modifica o sentido da mensagem original

Figura 5 – Sistema de informação



Fonte: (SHANNON, 1948, p. 02)

causando, assim um erro de comunicação. Foi precisamente a identificação da presença do ruído interferindo na transmissão de mensagens que levou Shannon e seus companheiros à busca de uma solução para este problema, busca esta que também contribuiu no desenvolvimento dos códigos corretores de erros, cuja função é, como o nome já sugere, impedir através da correção de erros que a mensagem original tenha seu sentido distorcido após o seu envio.

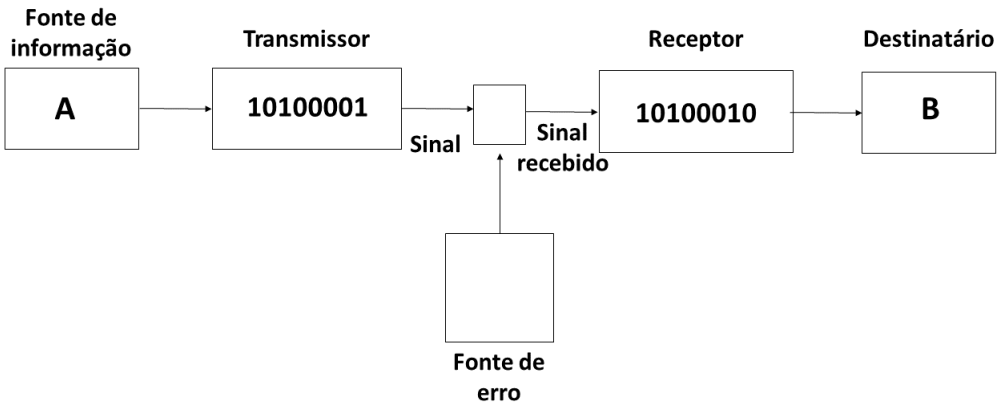
Vejamos um exemplo de como o erro afeta a transmissão de um símbolo do código ASCII e de como o diagrama de Shannon representa este fato.

Exemplo 2.1. Sabemos, pela Tabela 1, que no código ASCII, a letra A é codificada pelo símbolo 10100001 e a letra B por 10100010. Dessa forma, se em um sistema de informação, transmitirmos a letra A e por alguma interferência os últimos dois dígitos deste símbolo forem trocados, o destinatário receberá a letra B. Como este erro afeta a comunicação está ilustrado na Figura 6.

É instrutivo neste ponto, perceber que os sistemas de comunicação fazem parte do nosso dia a dia, bem como podem ser observados em situações que não estão diretamente relacionadas com computadores ou outros tipos de tecnologias ou equipamentos digitais[7]. Por exemplo, (GLEICK, 2013, p. 231) aponta que "No caso de uma conversa cotidiana, tais elementos são o cérebro do falante, as cordas vocais do falante, o ar, o ouvido do ouvinte e o cérebro do ouvinte". E, como todos já pudemos em algum momento perceber,

[7] Uma outra situação onde, olhando com cuidado, poderemos identificar elementos que compõem um sistema de informação e Códigos Corretores de Erros pode ser encontrado em (GLEICK, 2013, pp. 21 - 36), onde o autor nos conta como uma tribo africana se utilizava de tambores para se comunicarem por longas distâncias, em uma época em que o uso de tecnologias digitais como as conhecidas por nós estava fora de questão.

Figura 6 – Exemplo de erro



Fonte: O autor

este sistema também é afetado pelo ruído, pois, inúmeras são as situações onde não conseguimos entender nem nos fazer entender na comunicação com nossos pares, sejam por interferências que ocorrem no ambiente (um barulho que atrapalha uma conversa) ou por intereferências na nossa própria capacidade de compreender algo (entender errado uma palavra em uma conversa).

Outro exemplo de sistema de comunicação afetado pelo erro pode ser encontrado em (HARARI, 2016) que conta um mito do povo Igbo da Nigéria. Em suas palavras:

> [...] no início Chukwu, o deus da criação, quis fazer as pessoas imortais. Ele mandou um cão dizer aos humanos que deveriam borrifar o corpo dos mortos com cinzas, e com isso o corpo voltaria à vida. Infelizmente, o cão estava cansado e demorou-se no caminho. O impaciente Chukwu enviou então uma ovelha, dizendo-lhe que se apressasse em levar essa importante mensagem. Mas, quando chegou ao seu destino, a ofegante ovelha confundiu as instruções e disse aos humanos que enterrassem seus mortos; por essa razão a morte tornou-se permanente. (HARARI, 2016, pp. 55 - 56).

Neste caso, temos o deus Chukwu como *uma fonte de informação*, a ovelha confusa ao mesmo tempo como *um transmissor* e *um canal*, a humanidade também ao mesmo tempo como *um receptor* e *um destinatário* da mensagem. Infelizmente neste caso, a ocorrência do erro levou a humanidade a conhecer a morte em vez da vida eterna.

Há ainda mais uma situação que gostaríamos de destacar, em que um sistema de informação pode ser facilmente identificado, neste caso, trazemos um exemplo da literatura, mais precisamente, do romance *Ensaio sobre a cegueira*, do escritor português, ganhador do Prêmio Nobel de Literatura, José Saramago. No trecho à seguir um grupo de pessoas cegas se encontram reunidas em um ambiente isolado do mundo exterior, cuja única fonte

de informações sobre o mesmo é um rádio pertencente a um dos cegos. O cego dono do rádio houve as notícias do jornal no rádio e

> [· · ·] Depois, com palavras suas, resumia as *informações* e *transmitia-as* aos vizinhos próximos. Assim, de cama em cama, as notícias iam lentamente dando a volta à camarata, *desfiguradas* de cada vez que passavam de um *receptor* ao *receptor* seguinte, diminuída ou agravada desta maneira a importância das *informações*, consoante o grau pessoal de optimismo e pessímismo próprio de cada *emissor*. (SARAMAGO, 1995, p. 150, itálicos nosso).

Neste exemplo, temos uma situação semelhante à brincadeira de criança conhecida como "Telefone sem fio", onde cada pessoa à partir do dono do rádio que é uma *fonte de informação* é simultaneamente um *receptor* e *transmissor*, além disso, a cada vez que a informação é transmitida de um cego para o outro, ela é acometida de *erro*, o qual é introduzido pela subjetividade dos indivíduos a cada nova transmissão.

Por fim, gostaríamos de notar que as contribuições de Shannon para o mundo tecnológico extrapolaram sua época e tem se mostrado tão significativas que o mesmo tem sido lembrado até hoje. Um exemplo disso foi a homenagem ao que seria o seu 100º aniversário, em cuja data, 30 de abril de 2016, foi publicado um Doodle na página inicial do Google. A Figura 7 mostra o Doodle com Shannon fazendo malabarismo[8] com os dígitos 0 e 1, tendo ao fundo um diagrama parecido com o presente na Figura 5, o qual se encontra em seu trabalho de 1948. O link para o Doodle pode ser acessado na nota abaixo[9].

Mais significativo ainda é o fato da Sociedade da Teoria da Informação - *Information Technology Society* no original, ter estabelecido o *Claude E. Shannon Award*[10], um prêmio destinado a pesquisadores que têm realizado contribuições significativas para este campo de estudo. O primeiro agraciado com este prêmio foi obviamente, o próprio Shannon em 1972 e desde então diversos pesquisadores da área têm sido honrados com o prêmio que faz a memória de Shannon permanecer viva.

---

[8] Shannon era conhecido entre seus colegas não apenas por seu trabalho, mas também por suas excentricidades, dentre as quais, estava a habilidade de fazer malabarismo e andar de monociclo, o que ele fazia nos corredores dos Laboratórios Bell, ver (GLEICK, 2013, p. 177). Seu interesse pela arte do malabarismo era tão grande que o mesmo foi capaz de construir máquinas que faziam malabares. Para os interessados, um vídeo destas máquinas e uma breve biografia da vida e obra de Shannon, podem ser encontrados, respectivamente em: <https://www.youtube.com/watch?v=sBHGzRxreJY.>, <https://medium.com/the-mission/10-000-hours-with-claude-shannon-12-lessons-on-life-and-learning-from-a-genius-e8b9297bee8f>.

[9] Doodle Claude Shannon: <https://www.google.com/doodles/claude-shannons-100th-birthday>

[10] Para maiores informações sobre este prêmio e esta sociedade ver: <https://www.itsoc.org/honors/claude-e-shannon-award>.

Figura 7 – Doodle em homenagem a Shannon

Fonte: Nota 9

2.3 Finais de semana perdidos

Outro nome importante ligado aos códigos corretores de erros é Richard Hamming, o qual, em abril de 1950, publicou no *The Bell System Technical Journal* o artigo *Error Detecting and Error Correcting Codes* (HAMMING, 1950), no qual conceitos fundamentais para a Teoria dos Códigos Corretores de Erros, como *métrica, redundância, equivalência de códigos e códigos sistemáticos*, por exemplo, foram primeiramente enunciados e abordados. Neste artigo, Hamming explica que a motivação para o estudo apresentado foi a necessidade que ele verificou de se resolver o problema que inevitavelmente surge no processamento de uma dada tarefa por uma máquina como um computador, a saber, os eventuais erros que ocorrem na realização da tarefa. Sobre o erro presente em um cálculo realizado por um computador, ele afirmou:

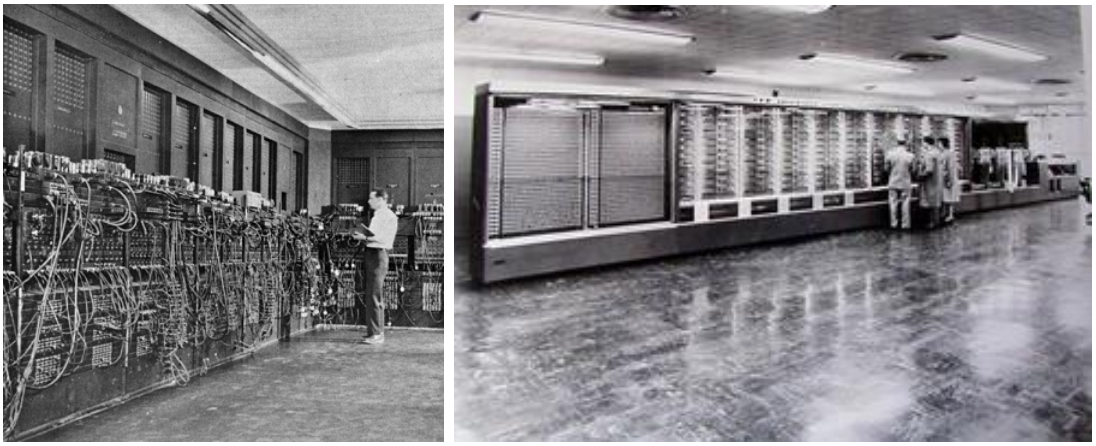
> [...] uma única falha geralmente significa o fracasso completo, no sentido de que se ela é detectada nenhum cálculo pode ser realizado até a falha ser localizada e corrigida, enquanto que se ela escapa da detecção então ela invalida todas as operações posteriores da máquina. (HAMMING, 1950, p. 147, tradução nossa).

Dessa forma, o operador ou usuário de tal máquina se vê diante de um impasse. Se um erro ocorrer e for detectado, então a máquina não funciona até o erro detectado ser corrigido, tarefa que na época não era realizada em pouco tempo e sem pouco trabalho. Por outro lado, se um erro ocorrer e não for detectado, os cálculos realizados não serão úteis, pois foram afetados pelo erro que comprometerá o resultado final de todo o trabalho realizado.[11]

[11] Situações semelhantes à descrita anteriormente, motivaram o meteorologista americano Edward Lorenz (1917 - 2008), a desenvolver, na década de 60, a teoria matemática que ficou popularmente conhecida como "Teoria do Caos". Suas descobertas ocorreram quando ele percebeu que os valores armazenados em seus cartões de memória e os valores armazenados e utilizados por seu computador em seus cálculos, diferiam em apenas algumas casas decimais, mas que mesmo estas pequenas diferenças faziam com que as previsões de seus modelos climáticos fossem totalmente transformadas. O ponto aqui é o fato de como pequenos erros ou disparidades de valores na realização de cálculos nos computadores da

Cabe aqui uma pequena pausa para salientarmos que as dificuldades enfrentadas pelos pesquisadores nessa época mostram como eles foram pioneiros e geniais em suas pesquisas, visto que o computador era algo extremamente novo para eles – o primeiro computador utilizado nos Estados Unidos data de 1946 e foi construído na Universidade da Pensilvânia a pedido das forças armadas (BLAINEY, 2011).

Figura 8 – Computadores da época: ENIAC à esquerda e MARK1 à direita.



Fonte: Google Images

A descrição de como o manejo dos computadores era trabalhoso e sobre como os erros afetavam este trabalho, pode ser vista na descrição a seguir:

> [. . .] quando se queria que um computador executasse alguma tarefa, eram necessários muitos cartões perfurados ou entregar uma fita aos operadores do computador, [...]. Isso era conhecido como "processamento por lote" era uma coisa aborrecida. Podia-se esperar por horas ou dias para obter os resultados; qualquer *erro mínimo* implicava recolocar os cartões perfurados para novo processamento e não se podia tocar e nem mesmo ver o computador propriamente dito. (ISSACSON, 2014, p. 238, itálico nosso).

Também nos salta aos olhos o fato de que pouco tempo após a publicação do artigo de Hamming, no ano de 1955 "[...] funcionavam cerca de 250 grandes computadores em todo o mundo, alguns dos quais ocupavam a área de uma ampla sala de estar. Feito de meio milhão de conexões soldadas à mão e necessitando de pelo menos 18 mil tubos de vácuo [...]". (BLAINEY, 2011, p. 230). Notando que estes eram os mais avançados computadores da época, para nós fica completamente justificada a crença e previsão, que felizmente posteriormente se mostrou errada, atribuída ao então diretor da IBM, Thomas

época causavam grandes erros, ou mesmo, invalidavam os trabalhos de quem sofria com os mesmos. Para uma introdução informal a este tema e ao resultado da descoberta de Lorenz ver o vídeo CAOS e EFEITO BORBOLETA, disponível em:<https://www.youtube.com/watch?v=C4eHJ8ZJgG4>

Jhon Watson (1874 - 1956) que teria afirmado, no inicio da década de 1940, que “no mundo inteiro não haveria mercado para mais do que cinco computadores”.[12]

Foi justamente neste novo e pouco explorado contexto que Hamming se encontrava em 1947 enquanto trabalhava com os computadores dos laboratórios Bell. Nesta época, a utilização dos computadores da empresa era obviamente limitada e disputada pelos pesquisadores da mesma, de forma que Hamming só tinha acesso aos mesmos nos finais de semana, e foi nestas pesquisas de “final de semana” que ele percebeu que as máquinas por ele utilizadas eram capazes de detectar os erros em sua programação, entretanto, isso não o ajudava em nada, pois as máquinas não possuíam a capacidade de corrigir tais erros.

Em entrevista dada em 1977, ele explica a situação em que se encontrava na época, e que em grande parte, foi um dos motivos que o levaram a trabalhar no desenvolvimento dos códigos corretores de erros. Ele afirma:

> Em dois finais de semanas consecutivos eu fui e descobri que todas minhas coisas tinham sido descarregadas e nada tinha sido feito. Eu estava realmente aborrecido e irritado porque queria estas respostas e tinha perdido dois finais de semana. E então eu me disse “Maldição, se as máquinas podem detectar um erro, porque não podemos localizar a posição do erro e corrigi-lo. (MILIES, 2009, p. 02).

Figura 9 – Richard Hamming

Fonte: Google Images

Vale notar que Hamming não era o único passando por situações como esta na

[12] Na realidade, não existem evidências escritas ou em outras formas de registro de que Watson de fato tenha dito esta frase, porém a frase passou para a posteridade como sendo própria de Watson. Para maiores detalhes, ver a biografia de Watson *The Maverick and His Machine: Thomas Watson, Sr. and the Making of IBM* de 2003, escrita por Kevin Maney.

época. Vejamos, a seguir, o depoimento de Robert Taylor[13] (1932 – 2017), falando sobre suas dificuldades com a detecção dos erros: “Eu tinha de ficar carregando pilhas de cartões que levavam dias para serem processados, e eles diziam que eu tinha posto uma virgula errada no cartão 653, ou algo do tipo, e eu precisava recomeçar tudo de novo, [...]. Isso me enfurecia.”. (ISSACSON, 2014, p. 245).

Diante disso tudo, com o intuito de manter viva a memória deste destacado pesquisador e pioneiro das tecnologias da comunicação, em 1986 o IEEE Instituto de Engenheiros Elétricos e Eletrônicos dos Estados Unidos ou *Institute of Eletrical and Eletronics Engineers* no original, estabeleceu a medalha Richard Hamming[14], como forma de premiar os pesquisadores de destaque na área da Ciêcia da Informação, sendo Hamming o primeiro a receber a medalha.

Figura 10 – Medalha Richard Hamming

Fonte: Google Images

2.4 Detectando e corrigindo erros

Ao ler o artigo de Hamming fica claro que era com o objetivo de compreender e fazer bom uso da correção de erros que ele passou a estudar o problema da detecção e correção de erros, uma vez que o problema da simples detecção de erros já estava resolvido na época, como ele mesmo afirma: “[...] parece desejável examinar o próximo passo além da detecção do erro, nomeadamente correção do erro.” (HAMMING, 1950, p. 148, tradução nossa).

Nesta seção e nas próximas trazemos os principais elementos de sua teoria, exposta no já citado artigo (HAMMING, 1950). Para desenvolver sua teoria, Hamming elabora alguns conceitos que o ajudarão nesta tarefa, a essência de tais conceitos está presente nas

[13] Robert Taylor foi um dos grandes nomes por trás do desenvolvimento da internet e do computador pessoal e nesta época também estava travando suas batalhas com a programação dos rudimentares computadores a sua disposição. Para uma breve introdução à sua vida e obra ver: <http://www.computerhistory.org/fellowawards/hall/robert-w-taylor/>

[14] Para mais informações sobre a medalha, o prêmio e os laureados com os mesmos ver: <https://www.ieee.org/about/awards/medals/hamming.html>.

Definições 2.2, 2.7 e 2.8 à seguir.

Definição 2.2. Sejam A um conjunto finito não vazio, o qual será chamamdo de alfabeto e $|A|$ o seu número de elementos. Um código corretor de erros C, é um subconjunto próprio qualquer de A^n, para algum n natural. Um elemento $c \in C$ é chamado um símbolo do código.

Da definição acima decorre que, dado um conjunto finito não vazio A qualquer, podemos, a partir dele, definir quantos códigos corretores de erros desejarmos, sendo tal construção limitada apenas por nossa criatividade e disposição. Vejamos alguns exemplos.

Exemplo 2.3. Se escolhermos como alfabeto o conjunto $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, temos que $|A| = 10$ e o conjunto $C \subset A^9$ formado por todos os números de celulares no Brasil é um Código Corretor de Erros.

Exemplo 2.4. Mais uma vez tomando como alfabeto o conjunto $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, temos que o seu número de identidade é um símbolo do conjunto $C \subset A^9$ que também é um Código Corretor de Erros.

Exemplo 2.5. Agora, se o conjunto A escolhido, for o nosso alfabeto, então o conjunto $C \subset A^{46}$, formado por todas as palavras do nosso idioma, também é um Código Corretor de Erros[15].

Exemplo 2.6. Os códigos de barras dos produtos que compramos, o registro de livros ISBN e o número do nosso CPF, são todos exemplos de Códigos Corretores de Erros cujo alfabeto também é $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e cujos símbolos estão no conjunto A^{13} para os dois primeiros e A^{11} para o último.

Uma pergunta que pode surgir após estes exemplos é: "Como corrigir os erros nestes códigos?". Esta pergunta não possui uma única resposta, por exemplo, nos três primeiros códigos acima, a repetição de um símbolo ao transmiti-lo, consiste num procedimento que permite a correção de erros, porém, a repetição nem sempre é o procedimento mais eficaz possível[16]. Já para os códigos citados no último exemplo existem procedimentos

[15] Neste exemplo estamos considereando que a maior palavra na língua portuguesa é Pneumoultramicroscopicossilicovulcanoconiótico, a qual, como pode ser vista, possui 46 letras. Para o significado desta palavra, bem como para conhecer outras palavras gigantescas como esta em outros idiomas, ver <https://mundoestranho.abril.com.br/curiosidades/qual-a-maior-palavra-do-portugues-e-de-outros-idiomas/>

[16] Como um exemlo, considere o caso de quando vamos passar um número de telefone para alguém. É comum, quando esta tranmissão não é feita pessoalmente, digamos quando é feita através de uma ligação, repetirmos o número duas vezes para que a pessoa que o está recebendo, confira se não

matemáticos um pouco mais sofisticados para a detecção e correção dos eventuais erros. Para os interessados em como estes procedimentos funcionam ver (SÁ; ROCHA, 2012).

Aqui surge a necessidade de se buscar procedimentos mais eficazes para a identificação e correção de erros, tarefa esta que nem sempre é simples, mais ainda, quando trabalhamos com alfabetos com muitos símbolos como os acima. Para resolver e evitar este tipo de problema Hamming escolhe trabalhar com códigos cujos símbolos sejam compostos por sequências numéricas contendo apenas 0's e 1's em seus dígitos[17], dos quais alguns serão utilizados para transmitir a informação desejada e outros serão utilizados para a detecção e correção de eventuais erros. Esta escolha nos leva para a próxima definição.

Definição 2.7. Sejam C um Código Corretor de Erros e n, m e k números naturais com $n > m$. Dizemos que C é sistemático quando cada símbolo de C tem exatamente n dígitos binários, dos quais m são associados com a informação, enquanto os $k = n - m$ dígitos restantes são utilizados para a detecção e correção de erros.

Ao se escolher trabalhar com códigos sistemáticos, nos vemos diante da seguinte pergunta: "Dados dois códigos sistemáticos C e C', como decidir qual dos dois é o mais eficiente?". Entendendo mais eficiente, por aquele que transmite a maior quantidade de informação m, dado um valor para o comprimento dos símbolos n, ou equivalentemente transmite uma determinada quantidade m de informação com o menor valor possível de n. Para responder esta pergunta, Hamming propôs a seguinte definição.

Definição 2.8. Sejam C um código e n e m naturais. A redundância R do código C é a razão entre o número de dígitos binários utilizados e o número mínimo necessário para transmitir a mesma informação, ou seja, $R = \frac{n}{m}$. Note que a redundância é um número maior ou igual a 1.

A partir de agora vamos trabalhar com códigos considerando a menor redundância, pois esta escolha é exatamente o que Hamming faz em seu artigo. Vale destacar que sempre é possível obtermos tais códigos, que chamaremos *códigos de redundância mínima*, uma

escreveu nenhum algarismo errado. Porém se estivermos abordando a transmissão de palavras tão grandes quanto a da nota anterior, este procedimento se torna pouco eficaz, pois é mais provavél que introduzamos mais erros na transmissão do que os corrijamos com este procedimento.

[17] Uma outra forma de apresentar esta condição foi dada por Irving S. Reed (1923 – 2012) e Gustave Solomon (1930 – 1996) em seu trabalho de 1960, intitulado *Polynomial codes over certain finite fields*, no qual eles definem um código corretor de erros como um mapeamento de um espaço vetorial sobre o corpo $\mathbb{Z}_2$ em outro espaço vetorial sobre o corpo $\mathbb{Z}_2$ de dimensão superior.

vez que, como será visto posteriormente, m e n sempre estão bem definidos. Além disso, salvo menção contrária, sempre usaremos $A = \{0, 1\}$[18].

Na primeira parte de seu artigo, Hamming apresenta a construção de códigos de redundância mínima em três casos específicos, a saber:

(1) Códigos *detectores* de um único erro;

(2) Códigos *corretores* de um único erro;

(3) Códigos *corretores* de um único erro além de *detector* de erros duplos.

Nas próximas subseções detalharemos os casos (1) e (2), o caso (3) não será considerado, pois o mesmo consiste simplemente na aplicação do algoritmo apresentado no caso (1) em um código elaborado conforme o algoritmo apresentado no caso (2). Dessa forma, no caso (3) corrigimos um erro e detectamos dois, um pelo algoritmo em (1) e um pelo algoritmo em (2). Em suma, sempte que falarmos nos códigos dos casos (1) e (2), teremos em mente as seguintes definições.

Definição 2.9. Um código C é dito detector de um único erro, quando na transmissão de um dado símbolo $c \in C$, um único erro ocorrido em apenas uma de suas posições pode ser detectado.

Definição 2.10. Um código C é dito corretor de um único erro, quando na transmissão de um dado símbolo $c \in C$, um único erro ocorrido em apenas uma de suas posições pode ser detectado e corrigido pela troca de 0 por 1 ou vice versa.

2.4.1 Códigos detectores de um único erro

Para o caso mais simples, ou seja, os códigos detectores de um único erro, Hamming propõe o seguinte algoritmo – chamado de *verificação de paridade* – para a codificação de um símbolo composto de uma lista com n 0's e 1's:

Algoritmo 2.11. Nas primeiras $n-1$ posições nós colocamos $n-1$ dígitos de informação. Na n-esima posição nós colocamos outro 0 ou 1, de modo que as n posições completas tenham um número par de 1's.

[18] Na maioria dos trabalhos atuais é comum representar o conjunto A como $\mathbb{Z}_2$. Na verdade, o conjunto $\mathbb{Z}_2$ quando munido de certas operações de soma $(+)$ e produto $(\cdot)$, satisfaz uma série de propriedades que o torna uma estrutura matemática conhecida como *corpo*. Neste trabalho evitamos enfatizar este aspecto do conjunto $\mathbb{Z}_2$, pois desejamos nos aproximar o máximo possível da abordagem original de Hamming, porém na Seção 2.6 ao abordar o código de Hamming de um ponto de vista matricial, definiremos o conjunto $\mathbb{Z}_2$ à partir de sua relação com o conceito de congruência módulo 2 ($\equiv mod 2$).

Note que isto é claramente um código detector de um único erro, uma vez que um único erro na transmissão deve levar a um número ímpar de 1's nos símbolos do código, o que nos permitirá concluir imediatamente que, de fato, a transmissão foi afetada pelo erro. Este código é atualmente denotado por $C(n, n-1)$ ou $C(n, m)$, em que n é a quantidade de posições dos símbolos do código e m é a quantidade de posições que contém a informação. Logo abaixo é possível observar um exemplo de como este algoritmo de codificação/decodificação funciona para o caso do código $C(8, 7)$.

Exemplo 2.12. Considerando a Tabela 2 a seguir, note que, com respeito aos 7 dígitos de informação, as duas primeiras linhas da tabela contêm um número ímpar de 1's. Portanto, antes de transmitir os símbolos 1000110 e 0010110 presentes nestas linhas, devemos adicionar, na 8ª posição destes, o dígito 1 para que a quantidade de 1's seja par, resultando nos símbolos codificados 10001101 e 00101101. Por outro lado, os símbolos nas duas últimas linhas contêm um número par de 1's nas 7 posições de informação. Assim, antes de transmitir os símbolos 0111010 e 1010011 presentes nestas linhas, devemos adicionar, na 8ª posição destes, o dígito 0 para que a quantidade de 1's seja par, resultando nos símbolos codificados 01110100 e 10100110. Dessa forma, se na transmissão o receptor receber um símbolo com um número ímpar de 1's, ele pode concluir que ocorreu um erro na transmissão.

Tabela 2 – Funcionamento do código $C(8, 7)$, detector de um único erro.

Dígitos de informação							**Dígito de verificação**
1	0	0	0	1	1	0	1
0	0	1	0	1	1	0	1
0	1	1	1	0	1	0	0
1	0	1	0	0	1	1	0

Fonte: O autor

Cabe aqui notar que, como $R = \frac{n}{m} = \frac{n}{n-1} = 1 + \frac{1}{n-1}$, poderíamos supor que, para obtermos uma redundância cada vez menor, deveríamos tornar o valor de n cada vez maior. Porém, o que ocorre ao se aumentar o valor de n é o indesejável aumento na probabilidade de ocorrência de erros na transmissão dos símbolos. Em suas palavras, Hamming explica: "[...] se $p \ll 1$ é a probabilidade de algum erro, então para n tão grande como $\frac{1}{p}$, a probabilidade de um símbolo correto é aproximadamente $\frac{1}{e} = 0,3679\ldots$, enquanto um erro duplo tem probabilidade $\frac{1}{2e} = 0,1839\ldots$." (ibid, p. 150). Como os erros duplos não são detectados por este código, ocorre que existe uma probabilidade de aproximadamente $18,4\%$ de surgirem erros duplos passando pelo sistema, ou seja, quase um em cada cinco símbolos sendo transmitidos com erros, e pior ainda, não detectados.

Antes de passar para o próximo tipo de código vale ressaltar que o código deste exemplo é, de acordo com a Definição 2.2, um subconjunto de A^8, em que A como já dissemos é o conjunto $\{0,1\}$. Além disso, a redundância deste código é $R = \frac{n}{m} = \frac{8}{7} \approx 1,14$ o que em termos práticos significa que a transmissão dos $2^7 = 128$ símbolos deste código após sua codificação é equivalente a transmissão de $128 \times \frac{8}{7} \approx 146$ símbolos do mesmo código se eles não fossem codificados. Por este motivo é que trabalhamos com códigos com redundância mínima, pois os mesmos possibilitam uma maior economia de dados na transmissão de uma dada informação.

2.4.2 Um primeiro passo na correção dos erros: códigos corretores de um único erro

No caso dos códigos corretores de um único erro, Hamming desenvolve dois algoritmos. Um será utilizado para a *codificação* e outro será utilizado para a *detecção, correção* e *decodificação* de uma sequência binária de n posições, das quais m são escolhidas para conter a informação e as outras k restantes, em que k é tal que $n = m + k$, são escolhidas para a *verificação de paridade*. A relação entre n, m e k, é dada pela Tabela 3, que apenas apresentamos e utilizamos aqui deixando sua construção para a Subseção 2.4.3 (Proposição 2.26). Os dois exemplos à seguir mostram como utilizar a Tabela 3 na prática.

Tabela 3 – Relação entre n, m e k.

n	m	k correspondente
1	0	1
2	0	2
3	1	2
4	1	3
5	2	3
6	3	3
7	4	3
8	4	4
9	5	4
10	6	4
11	7	4
12	8	4
13	9	4
14	10	4
15	11	4
16	11	5
	Etc.	

Fonte: (Hamming, 1950, p. 151)

Exemplo 2.13. Suponha que desejamos transmitir um símbolo do código ASCII (ver Tabela 1). Sabendo que os mesmos contêm 1 byte de informação ($m = 8$), consultamos

a Tabela 3, e verificamos que devemos adicionar quatro bits de informação redundante ($k = 4$) ao mesmo, de forma que o símbolo codificado terá doze posições ($n = 12$).

No próximo exemplo, adaptado de (HEFEZ; VILLELA, 2008, p. 02), mostramos como a Tabela 3 é utilizada na codificação de comandos para a movimentação de um robô que se move em 4 direções sobre um tabuleiro.

Exemplo 2.14. Considere um robô que se move sobre um tabuleiro quadriculado de modo que, ao darmos um dos comandos (Leste, Oeste, Norte ou Sul), o robô se desloca do centro de uma casa para o centro da casa contígua indicada pelo comando. Se definirmos estes comandos por: Leste $\longmapsto 00$, Oeste $\longmapsto 01$, Norte $\longmapsto 10$ e Sul $\longmapsto 11$, a Tabela 3 mostra que 2 dígitos de informação ($m = 2$), exigem 3 digitos de verificação ($k = 3$), logo, os símbolos codificados terão 5 posições ($n = 5$).

Uma possível codificação para estes comandos é a dada por: $00 \longmapsto 00\mathbf{0}0\mathbf{0}$, $01 \longmapsto 10\mathbf{01}\mathbf{1}$, $10 \longmapsto 11\mathbf{10}\mathbf{0}$ e $11 \longmapsto 01\mathbf{11}\mathbf{1}$. Em que os dígitos destacados em negrito (informação) são os comandos originais do robô pré-codificação, e os outros dígitos que aparecem sem negrito (redundância) estão todos em posições que são potências de 2. Esta não é a única forma de codificar os comandos do robô, mas como veremos à seguir (Algoritmo 2.15) é uma que permite a deteção e correção de um único erro. De fato, a ocorrência de um único erro antes da codificação, por exemplo, o envio de 00 ao invés de 01 faria com que o robô se movimentasse na direção oposta à que queríamos que ele fosse, porém, após a codificação, a ocorrência de um único erro não gera tal situação e mais ainda, é passível de ser corrigida como veremos a seguir.

Em um primeiro momento, o leitor pode pensar que a escolha desta codificação particular foi feita de forma arbitrária, mas ao contrário do que pode parecer, a mesma foi realizada seguindo um algoritmo definido em (HAMMING, 1950), o qual exemplificaremos a seguir e generalizaremos no Algoritmo 2.15.

Em seu algoritmo de codificação Hamming afirma que as posições de verificação devem estar localizadas em potências de dois, ou seja, as posições de verificação serão a 1ª, 2ª e 4ª, como vimos no Exemplo 2.14. Por questões de melhor entendimento, vamos chamar estas posições de v_1, v_2 e v_4 e destacaremos em negrito os símbolos $00, 01, 10, 11$, de sorte que tais símbolos, ao serem codificados, serão escritos como: $v_1v_2\mathbf{0}v_4\mathbf{0}$, $v_1v_2\mathbf{0}v_4\mathbf{1}$, $v_1v_2\mathbf{1}v_4\mathbf{0}$ e $v_1v_2\mathbf{1}v_4\mathbf{1}$. Para determinar v_1, v_2 e v_4, seguiremos o seguinte algoritmo:

- Para a codificação do símbolo $\mathbf{00}$ em $v_1v_2\mathbf{0}v_4\mathbf{0}$, v_1 será escolhido de forma que a soma $v_1 + \mathbf{0} + \mathbf{0}$ seja par, v_2 de forma que a soma $v_2 + \mathbf{0}$ seja par e v_4 de forma que

a soma $v_4 + \mathbf{0}$ seja par, logo, teremos $v_1 = 0, v_2 = 0$ e $v_4 = 0$ e o símbolo codificado será 00**0**0**0**.

- Para a codificação do símbolo **01** em $v_1v_2\mathbf{0}v_4\mathbf{1}$, v_1 será escolhido de forma que a soma $v_1 + \mathbf{0} + \mathbf{1}$ seja par, v_2 de forma que a soma $v_2 + \mathbf{0}$ seja par e v_4 de forma que a soma $v_4 + \mathbf{1}$ seja par, logo, teremos $v_1 = 1, v_2 = 0$ e $v_4 = 1$ e o símbolo codificado será 10**0**1**1**.

- Para a codificação do símbolo **10** em $v_1v_2\mathbf{1}v_4\mathbf{0}$, v_1 será escolhido de forma que a soma $v_1 + \mathbf{1} + \mathbf{0}$ seja par, v_2 de forma que a soma $v_2 + \mathbf{1}$ seja par e v_4 de forma que a soma $v_4 + \mathbf{0}$ seja par, logo, teremos $v_1 = 1, v_2 = 1$ e $v_4 = 0$ e o símbolo codificado será 11**1**0**0**.

- Para a codificação do símbolo **11** em $v_1v_2\mathbf{1}v_4\mathbf{1}$, v_1 será escolhido de forma que a soma $v_1 + \mathbf{1} + \mathbf{1}$ seja par, v_2 de forma que a soma $v_2 + \mathbf{1}$ seja par e v_4 de forma que a soma $v_4 + \mathbf{1}$ seja par, logo, teremos $v_1 = 0, v_2 = 1$ e $v_4 = 1$ e o símbolo codificado será 01**1**1**1**.

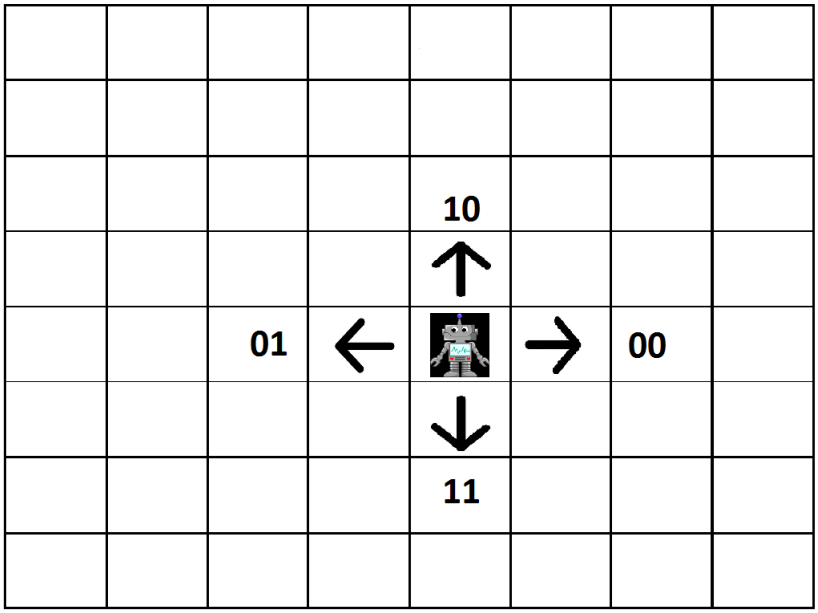
Assim, obtemos os símbolos codificados do Exemplo 2.14. Vejamos agora o caso geral para um símbolo $v_1v_2d_3v_4d_5d_6d_7v_8\cdots$ codificado à partir do símbolo $d_3d_5d_6d_7\cdots$.

Algoritmo 2.15. (Codificação) Para determinar v_1 some os valores dos dígitos nas posições $1, 3, 5, 7, \cdots$ de forma que a soma seja par[19], ou seja, "escolha" um dígito e "pule" um dígito à partir da 1ª posição. Para determinar v_2 some os valores dos dígitos nas posições $2, 3, 6, 7, 10, 11, \ldots$ de forma que a soma seja par, ou seja, "escolha" dois dígitos e "pule" dois dígitos à partir da 2ª posição. Para determinar v_4 some os valores dos dígitos nas posições $4, 5, 6, 7, 12, 13, 14, 15, \cdots$ de forma que a soma seja par, ou seja, "escolha" quatro dígitos e "pule" quatro dígitos à partir da 4ª posição. Este algoritmo continua até que sejam percorridas todas as posições nas potências de 2 do símbolo, sempre "escolhendo" e "pulando" dígitos nas potências de dois.

Suponha agora, que ao enviarmos o comando para o robô se movimentar para o norte, tenha ocorrido um erro e ao invés de ser transmitido o símbolo 11100 tenha sido transmitido o símbolo 11000, com um erro na terceira posição. Como verificar e corrigir este erro? Hamming nos responde com mais um algoritmo.

[19] Como os valores nas posições escolhidas serão sempre 0 ou 1, uma forma equivalente de enunciar este algoritmo seria postulando que a soma em questão seja congruente a 0 módulo 2. Porém para manter a abordagem do trabalho original de Hamming e também para desenvolvermos uma abordagem que se utilize apenas de conceitos vistos no Ensino Básico, decidimos não utilizar a idéia de congruência modular aqui, mas deixamos a mesma para ser abordada na Seção 2.6.

Figura 11 – Robô e comandos pré codificação



Fonte: O autor

Algoritmo 2.16. (Decodificação e correção) Vamos imaginar por um momento que temos recebido um símbolo de código, com ou sem um erro. Vamos aplicar as k verificações de paridade em ordem, e para cada vez que a verificação de paridade especificar o valor observado em sua verificação de posição nós escrevemos um 0, enquanto que para cada vez que os valores especificado e observado diferirem nós escrevemos um 1. Quando escrevermos da direita para a esquerda em uma linha, esta sequência de k 0's e 1's [...] pode ser considerada como um número binário e será chamado de um *número de verificação*. Vamos exigir que esse número de verificação dê a posição de um único erro, com o valor zero significando nenhum erro no símbolo. (HAMMING, 1950, p. 150, tradução nossa).

Vamos agora aplicar o Algoritmo 2.16 no símbolo 11000 e constatar que de fato o erro está na 3ª posição. Com efeito, para este símbolo temos $v_1 = 1, v_2 = 1$ e $v_4 = 0$, de maneira que:

- A primeira verificação de paridade atua nas posições $1, 3$ e 5, logo, nós temos que para $v_1 + 0 + 0$ ser par, v_1 tem que ser igual a zero, o que não confere com o valor de v_1, logo, esta verificação contribui com um 1 na sequência do número de verificação.

- A segunda verificação de paridade atua nas posições 2 e 3, de sorte que para $v_2 + 0$ ser par, v_2 tem que ser igual a zero, o que não confere com o valor de v_2, logo, esta verificação contribui com um 1 na sequência do número de verificação.

- A terceira e última verificação de paridade atua nas posições 4 e 5, de maneira que para $v_4 + 0$ ser par v_4 tem que ser igual a zero, o que confere com o valor de v_4, logo, esta verificação contribui com um 0 na sequência do número de verificação.

Escrevendo esta sequência como indicado, nós obtemos a sequência 011, que pode ser identificada com o número 011 na base 2, que é igual a 3 na base 10, logo o erro se encontra na 3ª posição, como já era de se esperar. Na Subseção 2.4.3 explicaremos com detalhes por que este algoritmo funciona e por que a sequência obtida representa, de fato, a posição onde se encontra o erro.

Vamos agora considerar um exemplo em que o robô do Exemplo 2.14 é atualizado para se movimentar em mais quatro direções.

Exemplo 2.17. Suponha que o robô do Exemplo 2.14 foi aprimorado, de forma que também seja possível movimentar o mesmo nas direções (Nordeste, Noroeste, Sudeste e Sudoeste). Se redefinirmos os comandos por: Leste $\longmapsto$ 000, Oeste $\longmapsto$ 010, Norte $\longmapsto$ 100, Sul $\longmapsto$ 110, Nordeste $\longmapsto$ 001, Noroeste $\longmapsto$ 011, Sudeste $\longmapsto$ 101 e Sudoeste $\longmapsto$ 111, o Algoritmo 2.15 e Tabela 3 (3 dígitos de informação $m = 3$, requerem 3 dígitos de verificação $k = 3$) nos fornecerão a seguinte codificação: 000 $\longmapsto$ 00**0**0**0**, 010 $\longmapsto$ 10**0**1**1**0, 100 $\longmapsto$ 11**1**0**0**, 110 $\longmapsto$ 01**1**1**1**0, 001 $\longmapsto$ 01**0**1**0**1, 011 $\longmapsto$ 11**0**0**1**1, 101 $\longmapsto$ 10**1**1**0**1 e 111 $\longmapsto$ 00**1**0**1**1, em que os dígitos destacados em negrito correspondem aos símbolos antes da codificação.

A forma de realizar a codificação destes símbolos é a mesma realizada no Exemplo 2.14, portanto não a repetiremos aqui. Entretanto, vamos apresentar uma forma mais direta para a verificação e correção do erro, ou seja, de aplicação do Algoritmo 2.16. Suponha que ao darmos o comando para o robô se movimentar na direção nordeste, o símbolo 010001 tenha sido transmitido ao invés do símbolo 010101, ou seja, ocorreu um erro na 4ª posição. Para detectar e corrigir este erro considere a Tabela 4 a seguir.

Tabela 4 – Correção de um erro

v_1	v_2	d_3	v_4	d_5	d_6	Número de Verificação
0	1	0	0	0	1	
0		0		0		0
	1	0			1	0
			0	0	1	1

Fonte: O autor

Na primeira linha da tabela rotulamos os dígitos que aparecerão nas colunas de 1 à 6 por v_1, v_2, d_3, v_4, d_5 e d_6, em que v_1, v_2 e v_4 são os dígitos de verificação e d_3, d_5 e d_6 são os dígitos de informação (os escritos em negrito no Exemplo 2.17). Na segunda linha da tabela, temos o símbolo que foi recebido na transmissão, a saber, 010001. Agora, note que os três zeros que aparecem na 3ª linha das seis primeiras colunas da tabela são os valores de v_1, d_3 e d_5 e que a soma de d_3 com d_5 é par e como $v_1 = 0$ esta verificação contribui com um 0 para o número de verificação (3ª linha e 7ª coluna). Prosseguindo a verificação, temos que a soma dos valores de d_3 e d_6 presentes na 4ª linha é ímpar e como $v_2 = 1$ esta verificação contribui com um 0 para o número de verificação. Finalmente, somando os valores de d_5 e d_6 na última linha obtemos resultado ímpar e como $v_4 = 0$ esta verificação contribui com um 1 para o número de verificação. Escrevendo o número de verificação em sua forma binária obtemos 100 que em escrita decimal é igual a 4, ou seja, o erro se encontra na 4ª posição, como era de se esperar.

Vejamos agora um exemplo, onde consideraremos o caso do envio de um símbolo sem erro e verificaremos que o Algoritmo 2.16 retorna, de fato, uma sequência contendo apenas zeros como indicação da não ocorrência de erro.

Exemplo 2.18. Seja $x = 01001110$ um símbolo pertencente a um código que transmite símbolos contendo um byte de informação, ou seja, $m = 8$. Para codificá-lo, consultamos a Tabela 3 e notamos que para este valor de m, devemos escolher $k = 4$ e $n = 12$, logo, o símbolo x ao ser codificado terá 12 posições. Após utilizarmos o Procedimento 2.15, obtemos o símbolo $x' = 100110011110$ codificação de x. Suponha que tal símbolo tenha sido transmitido corretamente, assim, ao utilizarmos o Procedimento 2.16 e calcularmos o número de verificação deste símbolo, devemos obter a sequência 0000, a qual indicará que não houve erro na transmissão. De fato, considerando a Tabela 5 abaixo, é fácil verificar que os valores dos dígitos na última coluna da mesma são de fato, todos iguais a zero.

Tabela 5 – Verificação da não ocorrência de erro

v_1	v_2	d_3	v_4	d_5	d_6	d_7	v_8	d_9	d_{10}	d_{11}	d_{12}	Número de Verificação
1	0	0	1	1	0	0	1	1	1	1	0	
1		0		1		0		1		1		0
	0	0			0	0			1	1		0
			1	1	0	0					0	0
							1	1	1	1	0	0

Fonte: O autor

Com estes exemplos encerramos a apresentação do código de Hamming em sua formulação original, a seguir mostraremos por que estes procedimentos de codificação e correção funcionam.

2.4.3 Por que o Procedimento 2.16 funciona e como obtemos a Tabela 3

A pergunta natural que surge nesse momento é: "Por que estes algoritmos de codificação e correção funcionam?". A resposta para esta pergunta pode ser encontrada na relação existente entre os números escritos nas bases 2 e 10, respectivamente. Para entender melhor o que estamos afirmando aqui, consideremos o teorema a seguir e o seu corolário mais adiante, cujas demonstrações podem ser encontradas em (HEFEZ, 2014, p. 68; 73), respectivamente.

Teorema 2.19. *Sejam dados os números inteiros a e b, com $a > 0$ e $b > 1$. Existem números inteiros $n \geqslant 0$ e $0 \leqslant r_0, r_1, \ldots, r_n < b$, com $r_n \neq 0$, univocamente determinados, tais que $a = r_0 + r_1 b + r_2 b^2 + \cdots + r_n b^n$.*

Note que este teorema garante que podemos escrever um número a dado, na base $b > 1$ que preferirmos. Em particular, quando $b = 10$, dizemos que o número a está escrito na base 10 ou em sua expansão decimal e escrevemos $(a)_{10}$, enquanto que quando $b = 2$, dizemos que o número a está escrito na base 2 ou em sua expansão binária e escrevemos $(a)_2$.

Exemplo 2.20. Quando a base $b = 60$, nós obtemos o sistema de numeração utilizado pelos antigos babilônios, chamado de sistema sexagesimal. Deste sistema herdamos a forma de representação de ângulos e seus submúltiplos, bem como das horas e seus submúltiplos.

O corolário a seguir nos permite relacionar um número em sua representação na base 10 com a sua respectiva representação na base 2 e vice-versa. Tal relação, embora não tenha sido explicitada, está no cerne dos algoritmos de codificação, decodificação e detecção de erro desenvolvidos por Hamming.

Corolário 2.21. *Todo número natural a escreve-se de modo único como soma de potências distintas de 2, a saber, $a = r_n \times 2^n + r_{n-1} \times 2^{n-1} + \ldots r_1 \times 2^1 + r_0 \times 2^0$, com $r_i \in \{0, 1\}$.*

Vejamos alguns exemplos simples de aplicação deste corolário.

Exemplo 2.22. Segundo o corolário anterior, o número $(739)_{10}$ é escrito, utilizando-se apenas potências de 2, como $1 \times 2^9 + 0 \times 2^8 + 1 \times 2^7 + 1 \times 2^6 + 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$. Ou de forma mais sucinta $(739)_{10} = (1011100011)_2$.

Exemplo 2.23. Também pelo corolário anterior, temos que $(100110)_2 = 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0 = (38)_{10}$.

O próximo exemplo é um caso dentre as muitas curiosidades sobre números e bases numéricas que podemos facilmente encontrar na internet[20].

Exemplo 2.24. O número π escrito na base 2, até a sua 100ª casa decimal, é igual a $\pi = 11,0010010000\ 1111110110\ 1010100010\ 0010000101\ 1010001100\ 0010001101\ 0011000100\ 1100011001\ 1000101000\ 1011100000$.

O exemplo a seguir é bastante esclarecedor para a compreensão do Algoritmo 2.16, bem como será útil mais adiante no Capítulo 3, quando apresentarmos uma sequência didática para o ensino de Códigos Corretores de Erros.

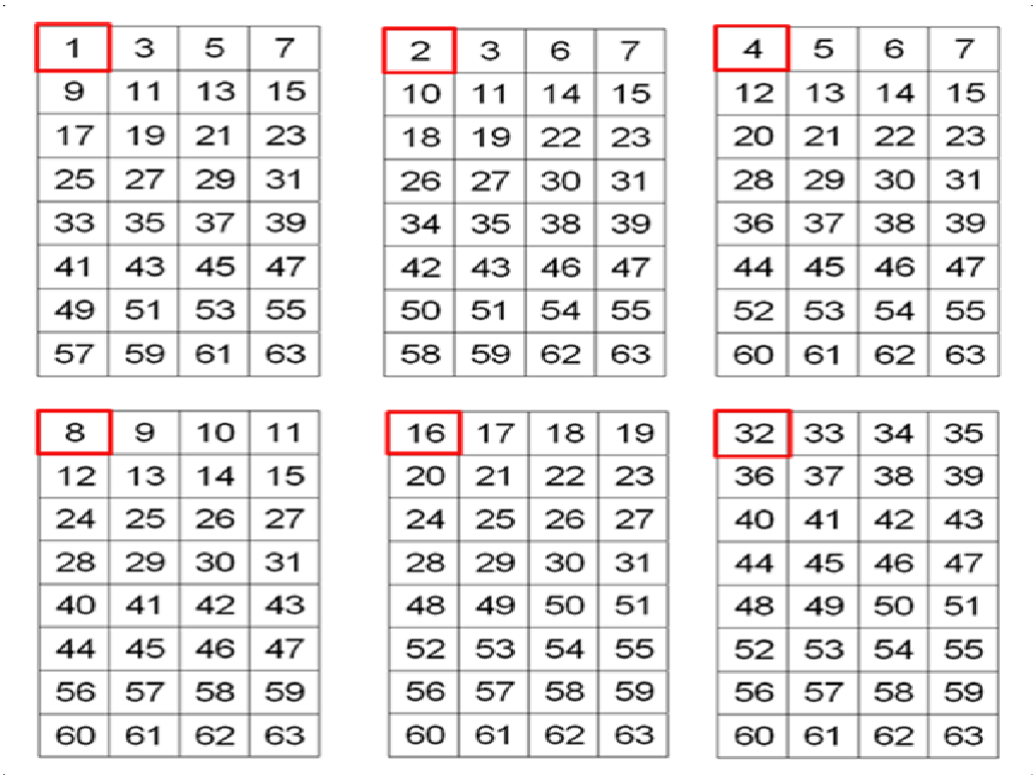
Exemplo 2.25. Note que os cartões da Figura 12, podem ser utilizados para representar qualquer número natural entre 1 e 63 como a soma de potências de dois. Note também que a obtenção do número 39, por exemplo, é feita escolhendo os cartões que começam com $1, 2, 4$ e 32, respectivamente, ou seja, $39 = 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$ ou se preferirmos $(39)_{10} = (100111)_2$, como também estes cartões são os únicos onde figura o número 39.

Perceba porém, que o que fizemos no Exemplo 2.25 é exatamente o que Hamming faz no Algoritmo 2.16. De fato, no Algoritmo 2.15 (para codificar um símbolo) Hamming escolhe somar os dígitos nas posições $1, 3, 5, 7, 9, 11, 13, 15\ldots$ na obtenção de v_1, somar os dígitos nas posições $2, 3, 6, 7, 10, 11, 14, 15\ldots$ na obtenção de v_2, somar os dígitos nas posições $4, 5, 6, 7, 12, 13, 14, 15\ldots$ na obtenção de v_4, e assim por diante. Estes números que aparecem aqui são exatamente os que figuram nos 1º, 2º e 3º cartões da Figura 12, respectivamente. Desta forma ao obter $v_1, v_2, v_4, \ldots$ por este algoritmo Hamming "prepara o caminho" para a utilização do Algoritmo 2.16.

Com efeito, de acordo com o Algoritmo 2.16, se o valor obtido na primeira verificação coincidir com o valor de v_1 escrevemos um 0, caso contrário, escrevemos um 1, semelhantemente, procedemos para $v_2, v_4, \ldots$ até percorrermos todas as posições de verificação do símbolo. Desta forma, ao obtermos a sequência de k $0's$ e $1's$ ao final do cálculo envolvendo todas as posições de verificação, ela de fato, representará um número

[20] O site consultado para este exemplo pode ser acessado em <http://wims.unice.fr/wims/es_tool~number~baseconv.es.html>

Figura 12 – Cartões para obter um número natural entre 1 e 63



1	3	5	7
9	11	13	15
17	19	21	23
25	27	29	31
33	35	37	39
41	43	45	47
49	51	53	55
57	59	61	63

2	3	6	7
10	11	14	15
18	19	22	23
26	27	30	31
34	35	38	39
42	43	46	47
50	51	54	55
58	59	62	63

4	5	6	7
12	13	14	15
20	21	22	23
28	29	30	31
36	37	38	39
44	45	46	47
52	53	54	55
60	61	62	63

8	9	10	11
12	13	14	15
24	25	26	27
28	29	30	31
40	41	42	43
44	45	46	47
56	57	58	59
60	61	62	63

16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

32	33	34	35
36	37	38	39
40	41	42	43
44	45	46	47
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

Fonte: Google Images

escrito na base 2, pois escrever um 0 ou um 1 em cada etapa implica em escolher ou não um dos cartões da Figura 12, e tal escolha, significa tão somente escrever um número natural como a soma de potências de dois.

Outra forma de perceber isto, é notar que ao obtermos um valor diferente do de v_1 na primeira verificação, podemos concluir que ocorreu um erro em uma das posições $1, 3, 5, 7, 9, 11, 13, 15 \ldots$, ao obtermos um valor diferente do de v_2 na segunda verificação, podemos concluir que ocorreu um erro em uma das posições $2, 3, 6, 7, 10, 11, \ldots$, e assim procedemos com $v_4, v_8, \ldots$ até percorrermos todas as posições de verificação. Suponha, por exemplo, que em uma verificação, obtemos a seguinte sequência 0101, ou seja, na verificação de v_1, v_2, v_4 e v_8 obtivemos valores não coincidentes na verificação de v_1 e de v_4, olhando para os cartões da Figura 12, note que o único número que está ao mesmo tempo no primeiro e terceiro cartões é 5, que por sua vez, quando escrito na base 2 é igual a 0101, logo, neste caso, ocorreu um erro na 5ª posição.

Para encerrar esta seção vamos mostrar como os valores de n, m e k presentes na Tabela 3 foram obtidos. Para isso, considere a seguinte proposição que relaciona o número de verificação com os valores de n, m e k.

Proposição 2.26. *Sejam $C \in A^n$, um código corretor de erros e n, m e k naturais, tais*

que m é o número de posições de informação, k é o número de posições de verificação dos símbolos do código e $n = m + k$. Vale a seguinte relação entre n e m: $\frac{2^n}{n+1} \geqslant 2^m$.

Demonstração. De fato, note que o número de verificação deve descrever $m + k + 1$ possibilidades diferentes, a saber, $n = m + k$ posições que dizem respeito a um erro em qualquer posição no símbolo, mais uma possibilidade no caso da não existência de erro. Isso implica na necessidade de ser $2^k \geqslant m+k+1$, uma vez que 2^k é o número de sequências com k posições contendo apenas $0's$ e $1's$. Utilizando o fato de que $n = m + k$ obtemos $2^{n-m} \geqslant n + 1 \Rightarrow \frac{2^n}{2^m} \geqslant n + 1 \Rightarrow \frac{2^n}{n+1} \geqslant 2^m$, o que prova o resultado.

Com esta proposição concluímos que atribuindo valores para n, ou seja, escolhendo a quantidade de posições que os símbolos de C possuirão, a inequação acima nos fornece o maior valor possível para m, ou seja, a maior quantidade de posições de informação que os símbolos de C possuirão. Por outro lado, feita a escolha de m a mesma inequação nos fornece o menor valor para n, ou seja, os símbolos com menor tamanho para o código C contendo uma certa quantidade de informação. Dessa forma, a inequação acima nos permite escrever o código que carregue a maior quantidade de informação possível com a maior economia possível.

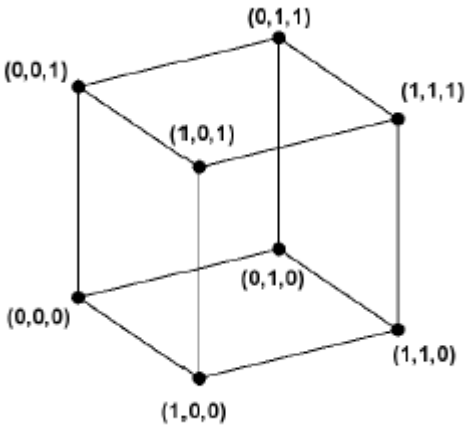
Note que se no lugar de considerarmos a inequação $2^k \geqslant m + k + 1$, como fizemos anteriormente, nós considerarmos apenas a igualdade $2^k = m + k + 1$, ou seja, se o número de verificação nos der exatamente $m + k + 1$ posições diferentes e sabendo que $n = m + k$, segue que $m = 2^k - k - 1$ e $n = 2^k - 1$. Logo, ao representarmos um código de Hamming na forma $C(n, m)$ o mesmo será descrito por $C(2^k - 1, 2^k - k - 1)$ e é justamente para esta família de códigos que daremos uma abordagem matricial na Seção 2.6. Códigos que satisfazem esta condição são ditos *perfeitos*. Para demonstrações do fato que o código de Hamming é perfeito, ver (HEFEZ; VILLELA, 2008, p.100) ou (SHINE, 2009, p. 301).

2.5 Uma interpretação geométrica

Após nos apresentar o seu código, Hamming propõe uma interpretação geométrica para o mesmo. A ideia concebida para o modelo geométrico do código de Hamming, consiste em identificar os símbolos de um código com alguns dos vértices de um cubo unitário n-dimensional. Note que o cubo unitário n-dimensional possui 2^n vértices, enquanto que um código com símbolos codificados contendo n posições possui 2^m símbolos, uma vez que os códigos $C(n, m)$ codificam 2^m símbolos, com $m < n$. Assim, um código corretor de erros nesta interpretação geométrica consiste de um subconjunto do cubo unitário n-dimensional contendo até 2^m elementos.

Vejamos como podemos construir um código detector de um único erro utilizando esta ideia, para isso consideremos as definições de distância entre dois pontos do cubo unitário n-dimensional e de esfera em um cubo unitário n-dimensional.

Figura 13 – Cubo unitário tridimensional.



Fonte: O autor

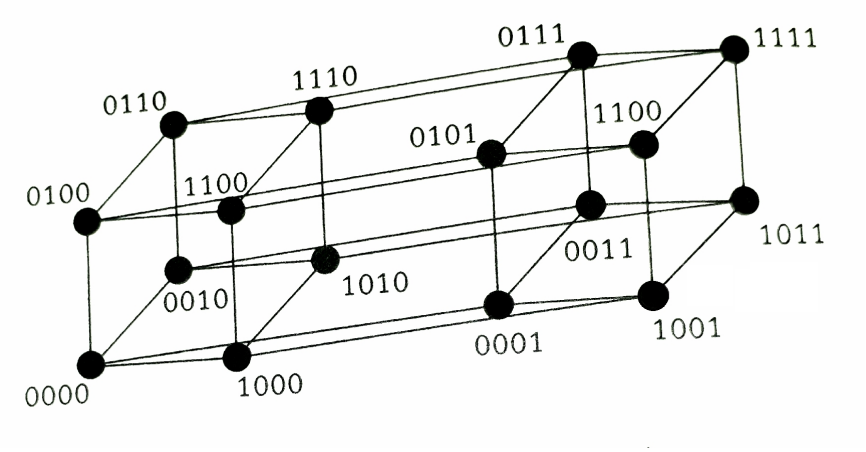
Definição 2.27. A distancia $D(x, y)$ entre dois pontos x e y do cubo unitário n-dimensional é igual ao número de posições para as quais as coordenadas de x e y são diferentes.

Observando a Figura 13, é possível ver que a distância entre dois pontos x e y quaisquer do cubo unitário tridimensional é igual ao número mínimo de arestas que devem ser percorridas para ir de x a y.

Exemplo 2.28. A distância entre os pontos $x = 010$ e $y = 101$ pertencentes ao cubo unitário tridimensional é $D(010, 101) = 3$, pois existem três posições para as quais as coordenadas de x e y são diferentes. Da mesma forma pode-se verificar que partindo de x são necessários no mínimo três movimentos pelas arestas do cubo unitário tridiminsional para chegar a y.

Vale ressaltar aqui que, embora não seja uma tarefa simples, segundo (STEWART, 2013) é possível desenhar e visualizar o cubo unitário n-dimensional para valores de n maiores do que 3. Este mesmo autor apresenta uma representação no plano do cubo unitário quadridimensional, a qual reproduzimos na Figura 14.

Figura 14 – Cubo unitário quadridimensional.



Fonte: (STEWART, 2013, p. 330)

Exemplo 2.29. A distância entre os pontos $x = 0010$ e $y = 1111$ do cubo unitário quadridimensional é $D(0010, 1111) = 3$, pois existem três posições para as quais as coordenadas de x e y são diferentes. De forma semelhante, observa-se que partindo de x são necessários pelo menos três movimentos pelas arestas do cubo unitário da Figura 14 para chegar a y.

O mais notável da definição de distância dada por Hamming é o fato dela possuir as três propriedades que caracterizam uma *métrica*, como podemos ver na próxima proposição.

Proposição 2.30. *Sejam x, y e z pontos do cubo unitário n-dimensional. A distância de Hamming possui as seguintes propriedades:*

i) $D(x, y) = 0$ *se, e somente se,* $x = y$*;*

ii) $D(x, y) = D(y, x) > 0$ *se* $x \neq y$

iii) $D(x, z) \leq D(x, y) + D(y, z)$ *(desigualdade triangular).*

Demonstração. As propriedades i) e ii) são de verificação imediata, pois a distância entre um ponto do cubo n-dimensional até ele mesmo é zero seja qual for este ponto, além disso, o percurso realizado partindo do ponto x e chegando no ponto y é igual ao partindo de y para x. Para iii) considere $x = x_1x_2 \ldots x_n$, $y = y_1y_2 \ldots y_n$ e $z = z_1z_2 \ldots z_n$, três pontos do cubo unitário n-dimensional e note que a contribuição das i-ésimas coordenadas de x e z para $D(x, z)$ é zero ou um, caso $x_i = z_i$ ou $x_i \neq z_i$, respectivamente. Daí segue que no caso $x_i = z_i$, tem-se que a contribuíção da i-esima coordenada para $D(x, z)$ é zero e consequentemente $D(x, z) \leq D(x, y) + D(y, z)$. No caso $x_i \neq z_i$ não podemos ter $x_i = y_i$ e $y_i = z_i$ simultaneamente, logo, a contribuição das i-ésimas coordenadas a $D(x, y) + D(y, z)$

é pelo menos um, o que prova o resultado.

Exemplo 2.31. Dados os símbolos $x = 0001, y = 1100$ e $z = 1111$ pertencentes ao cubo quadridimensional, verifiquemos que $D(x, z) \leq D(x, y) + D(y, z)$. De fato, $D(x, z) = 3$, por sua vez, $D(x, y) = 3$ e $D(y, z) = 2$, logo, $3 = D(x, z) \leq D(x, y) + D(y, z) = 3 + 2$.

Imediatamente derivado do conceito de métrica temos o conceito de *esfera*, o qual é definido como segue.

Definição 2.32. Sejam r um número natural e x um ponto do cubo unitário n-dimensional. Uma esfera de raio r ao redor do ponto x é definida como o conjunto formado por todos os pontos do cubo unitário n-dimensional que estão a uma mesma distancia r do ponto x.

Nos exemplos à seguir definimos algumas esferas abitrariamente. As esferas definidas nos dois primeiros exemplos podem ser facilmente visualizadas através das Figuras 13 e 14, entretanto, a esfera do terceiro infelizmente não pode ser visualizada, mas o fato relevante aqui é a sua adequação à Definição 2.32, uma vez que mesmo as esferas dos primeiros dois exemplos não têm a aparência de esferas como comumente as imaginamos.

Exemplo 2.33. Considerando os pontos do cubo unitário tridimensional da Figura 13, nós temos que a esfera com centro em 101 e raio $r = 1$ consiste dos pontos: $001, 111$ e 100, visto que estes estão a uma distância $D = 1$ do ponto 101.

Exemplo 2.34. Considerando os pontos do cubo unitário 4-dimensional, nós temos que a esfera com centro em 1010 e raio $r = 2$ consiste dos pontos: $0000, 0110, 1100, 1001, 0011$ e 1111.

Exemplo 2.35. Considerando os pontos do cubo unitário 5-dimensional, nós temos que a esfera com centro em 00000 e raio $r = 3$ consiste dos pontos: $11100, 01110, 10110, 11010,$ $10011, 01011,$ $00111, 11001,$ 10101 e 01101.

Vejamos como um código detector de um único erro pode ser obtido à partir destes conceitos.

Exemplo 2.36. Considere o cubo unitário tridimensional da Figura 13, e nele tome os pontos que distam duas unidadse do ponto 000. Estes pontos são: $011, 101$ e 110, os quais

definem uma esfera de raio $r = 2$ e centro 000 no cubo unitário tridimensional. Estes pontos também definem um código detector de um único erro, uma vez que um único erro cometido em qualquer posição destes vai resultar em um ponto que não pertence à esfera, logo, podemos concluir que houve um erro na trasmissão do mesmo.

Note que os elementos que definem a esfera deste exemplo são os mesmos símbolos que codifcam os comandos do robô do Exemplo 2.14, na Seção 2.4 codificados para a detecção de um único erro, obtidos através do Algoritmo 2.11.

Vejamos mais um exemplo de como o conceito de esfera pode ser utilizado na construção de um código detector de um único erro.

Exemplo 2.37. Considere o cubo unitário quadridimensional da Figura 14. O mesmo, como pode se ver, é composto de $2^4 = 16$ pontos, destes, tomemos os que estão sob a superfície da esfera de raio $r = 2$ e centro 0000. Tais pontos são: $1010, 1100, 0110, 0011, 0101$ e 1001, os quais juntamente com 000, compõem um código detector de um único erro, visto que a mudança de um único dígito de qualquer posição de um destes símbolos (pontos da esfera) faz com que o mesmo não esteja na esfera. Note que o ponto 1101, por exemplo, pertence ao cubo unitário, mas não pertence à esfera, pois, $D(0000, 1101) = 3$, logo o recebimento do mesmo em uma transmissão indicará um erro ocorrido, sem contudo corrigir tal erro.

De forma semelhante ao que foi visto após o Exemplo 2.36, os símbolos da esfera $1010, 1100,\ 0110, 0011, 0101$ e 1001 e seu centro 0000, são os mesmos que obteríamos utilizando o Algoritmo 2.11 para codificação dos símbolos $101, 110, 011, 001, 010, 100$ e 000. Além disto, este código não é capaz de corrigir um eventual erro, mas apenas de detectá-lo. De fato, o símbolo 1101 por exemplo, pode ter sido o resultado do erro na transmissão de um dos símbolos $1100, 1001$ ou 0101, pois todos diferem de 1101 em apenas uma coordenada.

Para construir um código corretor de um único erro, Hamming afirma que devemos escolher os símbolos do cubo unitário n-dimensional que estejam distanciados uns dos outros em uma distância de pelo menos três unidades. Mais ainda, ele observa que

> Se todos os pontos de código estão a uma distância de no mínimo 2 uns dos outros, então segue-se que um único erro levará um ponto de código a um ponto que não é um ponto de código, e portanto um símbolo sem significado. Isto por sua vez significa que um único erro é detectável. Se a distância mínima entre os pontos de código é pelo menos três unidades então qualquer único erro vai deixar o ponto mais perto do ponto do código correto que qualquer outro ponto do código, e isto significa que qualquer único erro será corrigível. (HAMMING, 1950, p. 155, tradução nossa).

Estas observações nos levam a um resultado mais geral relacionando a distância entre os pontos de um código e a sua capacidade de detecção e correção de erros. Para chegarmos a este resultado precisaremos da seguinte definição.

Definição 2.38. Seja C um código. A distância mínima de C é o número $d = min\{D(x, y); x, y \in C \text{ e } x \neq y\}$. Ou seja é a menor das distâncias entre os pontos do código.

Note que distância mínima está bem definida, pois é o menor elemento de um conjunto não vazio de números naturais, o qual sempre existe, segundo Princípio da Boa Ordenação[21], tal conjunto sempre possuirá um menor elemento, visto que o mesmo é não vazio.

É fácil verificar que o código do Exemplo 2.37 tem distância mínima $d = 2$. O resultado que relaciona a distância mínima de um código e a sua capacidade de detecção e correção de erros está presente na seguinte proposição, cuja demonstração pode ser encontrada em (HEFEZ; VILLELA, 2008, p. 07).

Proposição 2.39. *Seja C um código com distância mínima d. Então C pode corrigir até $[\frac{d-1}{2}]$ erros e detectar até $d-1$ erros. Onde $[\frac{d-1}{2}]$ representa a parte inteira do número $\frac{d-1}{2}$.*

Ao considerarmos diferentes valores para d, a proposição anterior nos dá o significado da distância mínima e o seu papel na construção de códigos detectores e corretores de erros. Estes resultados estão sintetizados na Tabela 6.

Tabela 6 – Distâncias mínimas e seus significados

Distância mínima	Significado
1	não corrige, nem detecta erro
2	não corrige, mas detecta um único erro
3	corrige um único erro e detecta até dois erros
4	corrige um erro e detecta até três erros
5	corrige até dois erros e detecta até quatro erros
⋮	⋮

Fonte: O autor

[21] Para uma exposição do Princípio da Boa Ordenação ver, por exemplo, o clássico livro *Um curso de Análise, vol. 1* do professor Elon Lages Lima.

Exemplo 2.40. Os pontos do cubo unitário 5-dimensional $00000, 10011, 11100$ e 01111 têm distância mínima igual a 3, logo, definem um código corretor de um único erro e detector de até dois erros. Supondo que na transmissão do símbolo 10011 ocorreu um erro na quarta posição, o símbolo recebido será 10001. Para corrigí-lo, basta calcular sua distância em relação aos outros símbolos do código e verificar qual o mais próximo dele, este é o símbolo que deveria ser enviado. Neste caso, temos $D(10001, 00000) = 2, D(10001, 10011) = 1, D(10001, 11100) = 3, D(1001, 01111) = 4$, como a menor destas distâncias é entre 10001 e 10011 segue que o símbolo com erro foi 10011, pois este difere do recebido em apenas uma posição, a saber, a posição em que ocorreu o erro.

Note que, ainda obtemos códigos corretores de um único erro e detector de até dois, se realizarmos as seguintes operações: i) permutarmos a primeira e a terceira posição; ii) trocarmos $0's$ por $1's$ ou $1's$ por $0's$ em todas as posições; iii) trocarmos $0's$ por $1's$ $1's$ por $0's$ nas quartas posições de cada um destes símbolos. De fato, após estas operações, obtemos os conjuntos: $\{00000, 00111, 11100, 11011\}$, $\{11111, 01100, 00011, 10000\}$ e $\{00010, 10001, 11110, 01101\}$, respectivamente, os quais também possuem distância mínima igual a 3. Logo, também definem todos, um código corretor de um único erro e detector de até dois.

Como pela Proposição 2.39 um código corretor de erros C qualquer, pode ser caracterizado em termos de sua distância mínima, podemos pensar em códigos que possuem símbolos diferentes, mas que não diferem em essência. Tais códigos são chamados de códigos equivalentes. A definição a seguir caracteriza dois códigos equivalentes.

Definição 2.41. Dois códigos C e C' são ditos equivalentes, se através de um número finito das seguintes operações um pode ser transformado no outro:

i) A permutação de quaisquer duas posições em todos os símbolos do código.

ii) O complementar (ou a troca de $0's$ por $1's$ e vice versa) dos valores em qualquer posição nos símbolos do código.

Dessa forma, podemos concluir que os códigos $C = \{00000, 10011, 11100, 01111\}$, $C' = \{00000, 00111, 11100, 11011\}$, $C'' = \{11111, 01100, 00011, 10000\}$ e $C''' = \{00010,$ $10001,\ 11110, 01101\}$ são equivalentes. Vejamos outro exemplo de códigos equivalentes.

Exemplo 2.42. No Exemplo 2.17 vimos que o código $C(6, 3) = \{000000, 100110, 111000,$ $011110, 010101, 110011, 101101, 001011\}$ fornece os comandos para a movimentação do

robô atualizado, com a detecção e correção de um único erro. Se aplicarmos a operação i) (permutar as primeiras e últimas posições), seguida da operação ii) (calcular o complementar em todas as posições) aos símbolos deste código, vamos obter o código $C'(6,3) = \{111111, 111000, 100110, 100001, 001011, 001100, 010010, 010101\}$, o qual é equivalente ao código $C(6,3)$ e ainda detecta e corrige um único erro, pois possui a mesma distância mínima de $C(6,3)$, a saber, $D = 3$.

Para encerrar esta seção, vamos mostrar como o código que definimos para o robô atualizado (Exemplo 2.17) se adequa a esta interpretação geométrica. De fato, os símbolos codificados dos comandos do robô atualizado são: $000000, 100110, 111000, 011110, 010101, 110011, 101101$ e 001011. É fácil ver que a distância mínima entre estes símbolos é igual a 3, de sorte que pela Tabela 6, este código é capaz de corrigir um único erro, vejamos como isso funciona. Suponha que ao trasmitirmos o símbolo 100110 tenha ocorrido um erro na segunda posição e o símbolo recebido tenha sido 110110. Para identificar o símbolo que deveria ser transmitido, basta calcular as distâncias entre o símbolo recebido 110110 e os símbolos do código, aquele que estiver mais próximo de 110110 é o símbolo que deveria ser enviado. Por outro lado, se ao calcularmos as distâncias entre o símbolo recebido e os símbolos do código e encontrarmos em alguma delas $D = 0$, isso significa que o símbolo foi enviado sem erro.

2.6 O código $C(7,4)$ e a famíla de códigos $C(2^k - 1, 2^k - k - 1)$

Agora que estudamos o código de Hamming em sua formulação original, daremos mais um passo em nosso estudo, apresentando uma formulação mais técnica do mesmo, utilizando ferramentas advindas da Teoria das Matrizes. Isto nos permitirá abordar posteriormente, na sequência didática, alguns conceitos estudados no Ensino Médio, como por exemplo, a multiplicação de matrizes e a transposta de uma matriz.

Com esse intuito, seguiremos de perto as ideias postas em (ROUSSEAU; AUBIN, 2015), fazendo as devidas modificações e alterações para tornar o texto mais claro. Dessa forma, trazemos uma teoria geral para os códigos $C(2^k - 1, 2^k - k - 1)$ paralelamente a uma visão particular sobre o código $C(7,4)$[22], onde os dígitos de informação são $m = 4$ e os de verificação são $k = 3$. Este código codifica todas as sequências binárias contendo 4 elementos, ou seja, $16 = 2^4$ símbolos, a saber, $0000, 0001, 0010, \cdots, 1111$. Nosso objetivo

[22] Já em seu artigo de 1948 (SHANNON, 1948, pp. 27 - 28), quando dava um exemplo de código eficiente, ou seja, um código que escolhido um valor para n é o que transmite a maior quantidade de informação possível, Shannon apresentava o código $C(7,4)$ de Hamming como um representante deste tipo de código. Mais ainda, a maneira que Shannon realizou a codificação deste tipo particular de código é a mesma feita nesta seção, exceto pelo uso das matrizes.

aqui é mostrar como funcionam a codificação, a decodificação e a correção de um único erro destes símbolos de uma forma diferente, porém equivalente a apresentada por Hamming em (HAMMING, 1950). A diferença aqui é que em vez de colocarmos os dígitos de verificação nas potências de 2, nós os colocaremos em posições diferentes destas, a saber, as últimas posições do símbolo, porém com a mesma verificação de paridade utilizada anteriormente na Seção 2.4.

Para deixarmos nossa exposição alinhada com a encontrada nos trabalhos atuais, vamos considerar com mais detalhes o papel do conjunto $\mathbb{Z}_2$ na construção destes códigos. Para isso, vamos construí-lo à partir da ideia de consgruência módulo 2. Para isso considere a seguinte definição.

Definição 2.43. Sejam a, b e m inteiros com $m > 1$. Dizemos que a e b são congruentes módulo m e denotamos $a \equiv b \ (mod\ m)$, quando a e b deixam o mesmo resto na divisão euclidiana por m.

Nos exemplos a seguir mostramos que os cálculos realizados com os inteiros considerando-se os seus restos, que convencionou-se chamar de *aritmética dos restos*, são bem parecidos com os cálculos realizados com os inteiros em si. Ou seja, podemos realizar as operações aritméticas com números congruentes módulo $m > 1$ sem muitas diferenças das operações aritméticas com os números usuais[23].

Exemplo 2.44. Os números 17 e -5 são congruentes módulo 11, pois deixam o mesmo resto na divisão por 11, a saber, 6. Representamos este fato escrevendo $17 \equiv -5 \ (mod\ 11)$.

Exemplo 2.45. Os números 107 e 32 são congruentes módulo 5, pois deixam o mesmo resto na divisão por 5, a saber, 2. Representamos este fato escrevendo $107 \equiv 32 \ (mod\ 5)$.

Exemplo 2.46. Note que $17 \equiv 13 \ (mod\ 4)$ e $57 \equiv 25 \ (mod\ 4)$, logo, $17 + 57 = 74 \equiv 38 = 13 + 25 \ (mod\ 4)$, pois, 74 e 38 deixam o mesmo resto na divisão euclidiana por 4, a saber, 2.

Exemplo 2.47. De forma semelhante ao exemplo anterior, note que $17 \equiv 13 \ (mod\ 4)$ e $57 \equiv 25 \ (mod\ 4)$, logo, $17 - 57 = -40 \equiv -12 = 13 - 25 \ (mod\ 4)$, pois -40 e -12 deixam o mesmo resto na divisão euclidiana por 4, a saber, 0.

[23] A única restrição que encontramos ao trabalharmos as operações aritméticas módulo $m > 1$ é com a divisão, porém não é nosso objetivo entrar em detalhes a este respeito. Para o leitor interessado neste assunto, ver (HEFEZ, 2014) ou (SANTOS, 1998). Nestes textos o leitor verá que os exemplos aqui mostrados são casos partículares de resultados mais gerais. Porém o conteúdo destes resultados está além do necessário para o nosso objetivo neste trabalho.

Exemplo 2.48. No caso da multiplicação, note que $17 \equiv 13\ (mod\ 4)$ e $57 \equiv 25\ (mod\ 4)$, logo, $17 \times 57 = 969 \equiv 325 = 13 \times 25\ (mod\ 4)$, pois 969 e 325 deixam o mesmo resto na divisão euclidiana por 4, a saber, 1.

Exemplo 2.49. Sabendo que $16 \equiv 9\ (mod\ 7)$ é fácil verificar que $16^3 = 4096 \equiv 729 = 9^3\ (mod\ 7)$, pois, 4096 e 729 deixam o mesmo resto na divisão euclidiana por 7, a saber, 1. Em geral, é facil mostrar que esta operação pode ser feita para qualquer inteiro $n > 1$.

Neste trabalho estamos interessados apenas no caso em que $m = 2$. Como o resto na divisão euclidiana de um número por 2 só pode ser 0 ou 1, nós podemos classificar todos os números inteiros em dois grupos (ou conjuntos): os números que deixam resto 0 estão reunidos no conjunto denotado por $\overline{0} = \{a \in \mathbb{Z};\ a \equiv 0\ (mod\ 2)\}$; os números que deixam resto 1 estão reunidos no conjunto denotado por $\overline{1} = \{a \in \mathbb{Z};\ a \equiv 1\ (mod\ 2)\}$. Note que $\overline{0} = \{\cdots, -4, -2, 0, 2, 4, \cdots\}$ e $\overline{1} = \{\cdots, -3, -1, 1, 3, \cdots\}$.

Usualmente o conjunto $\mathbb{Z}_2$ é representado como $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, porém por simplicidade, vamos denotá-lo simplismente por $\mathbb{Z}_2 = \{0, 1\}$ tendo sempre em mente que a soma de dois elementos de $\overline{1}$ resulta em um elemento de $\overline{0}$, pois, a soma de dois números que deixam resto 1 na divisão por 2 (ímpares) resultará em um número que deixa resto 0 na divisão por 2 (par). Assim podemos concluír que em $\mathbb{Z}_2$ vale a relação $1 + 1 = 0$.

Isto posto, vamos considerar o símbolo $x = 0101$ e ver como o codificar e o decodificar, além de corrigir um único erro em uma de suas posições.

Descrevendo os dígitos dos símbolos codificados da esquerda pra direita, os quatro primeiros serão os dígitos de informação d_1, d_2, d_3 e d_4 e os três últimos, os de verificação v_5, v_6 e v_7. O cálculo dos dígitos de verificação, e consequentemente sua codificação, é realizado através das iguadades: $v_5 = d_1 + d_2 + d_4$, $v_6 = d_1 + d_3 + d_4$ e $v_7 = d_2 + d_3 + d_4$, as quais explicaremos o motivo de serem assim mais adiante. Dessa forma, o símbolo codificado tem a representação $d_1d_2d_3d_4v_5v_6v_7$, onde v_5, v_6 e v_7 são como postos acima. Assim, para o símbolo $x = 0101$ temos que $d_1 = 0, d_2 = 1, d_3 = 0, d_4 = 1, v_5 = d_1+d_2+d_4, v_6 = d_1+d_3+d_4$ e $v_7 = d_2 + d_3 + d_4$. Logo, ao codificá-lo obtemos o símbolo $x' = 0101010$.

Note que na codificação dada pelo Algoritmo 2.15 o símbolo codificado tem a representação $v_1v_2d_3v_4d_5d_6d_7$, onde v_1 é escolhido de forma que a soma $v_1 + d_3 + d_5 + d_7$ seja par, v_2, de forma que a soma $v_2 + d_3 + d_6 + d_7$ seja par e v_4, de forma que a soma $v_4 + d_5 + d_6 + d_7$ seja par, o que é o mesmo que tomar

$$\begin{aligned} v_1 &= d_3 + d_5 + d_7 \\ v_2 &= d_3 + d_6 + d_7 \\ v_4 &= d_5 + d_6 + d_7. \end{aligned} \tag{2.1}$$

Daí segue que a codificação, agora escrita como $d_1d_2d_3d_4v_5v_6v_7$, é equivalente à codificação da Seção 2.4 escrita como $v_1v_2d_3v_4d_5d_6d_7$, onde a relação entre as duas codificações, quanto aos dígitos de verificação, é dada pela Tabela 7.

Note também que nesta forma de codificação a relação com a codificação da Seção 2.4 é a seguinte: v_5 faz o papel de v_1; v_6 faz o papel de v_2; v_7 faz o papel de v_4; e d_1, d_2, d_3 e d_4 fazem o papel de d_3, d_5, d_6 e d_7, respectivamente. Dessa forma, para codificar um símbolo do código $C(7,4)$, utilizamos o seguinte algoritmo.

Algoritmo 2.50. Para codificar um símbolo $d_1d_2d_3d_4v_5v_6v$ do código $C(7,4)$ utilize o Algoritmo 2.15 com a equivalência da Tabela 7.

Tabela 7 – Equivalência entre os digitos v_5, v_6 e v_7 e v_1, v_2 e v_4

Codificação na Seção 2.4	v_1	v_2	d_3	v_4	d_5	d_6	d_7
Codificação equivalente	v_5	v_6	d_1	v_7	d_2	d_3	d_4

Fonte: O autor

Vale destacar aqui que uma forma prática para codificar qualquer símbolo do código $C(7,4)$ é através da soma das colunas da Tabela 8. Assim, se considerarmos o símbolo $y = 0111$, por exemplo, temos $d_1 = 0, d_2 = 1, d_3 = 1$ e $d_4 = 1$, de modo que ao substituírmos estes valores na Tabela 8 e somarmos suas respectivas colunas, obteremos o símbolo codificado $y' = 0111001$.

Tabela 8 – Esquema para a codificação de um símbolo de $C(7,4)$

d_1	d_2	d_3	d_4	v_5	v_6	v_7
$1 \cdot d_1$	$0 \cdot d_1$	$0 \cdot d_1$	$0 \cdot d_1$	$1 \cdot d_1$	$1 \cdot d_1$	$0 \cdot d_1$
$0 \cdot d_2$	$1 \cdot d_2$	$0 \cdot d_2$	$0 \cdot d_2$	$1 \cdot d_2$	$0 \cdot d_2$	$1 \cdot d_2$
$0 \cdot d_3$	$0 \cdot d_3$	$1 \cdot d_3$	$0 \cdot d_3$	$0 \cdot d_3$	$1 \cdot d_3$	$1 \cdot d_3$
$0 \cdot d_4$	$0 \cdot d_4$	$0 \cdot d_4$	$1 \cdot d_4$	$1 \cdot d_4$	$1 \cdot d_4$	$1 \cdot d_4$

Fonte: O autor

Agora que já sabemos codificar um símbolo de $C(7,4)$, a pergunta que surge é: "Como decodificar e corrigir um erro de um símbolo deste código?". Para responder a esta pergunta, precisamos detectar se existe um erro e em qual posição, e corrigi-lo trocando 0 por 1 ou vice-versa, o que é feito de acordo com o seguinte algoritmo apresentado em (ROUSSEAU; AUBIN, 2015).

Algoritmo 2.51. Para detectar um possível erro, nós calculamos os dígitos de verificação do símbolo recebido, os quais denotaremos por w_5, w_6 e w_7 e depois os comparamos com os respectivos valores, nas posições de verificação, do símbolo recebido. Uma das seguintes possibilidades pode ocorrer:

1. $v_5 = w_5, v_6 = w_6$ e $v_7 = w_7$, neste caso o símbolo foi enviado sem erro;
2. $v_5 \neq w_5$ e $v_6 \neq w_6$, neste caso o erro está na primeira posição;
3. $v_5 \neq w_5$ e $v_7 \neq w_7$, neste caso o erro está na segunda posição;
4. $v_6 \neq w_6$ e $v_7 \neq w_7$, neste caso o erro está na terceira posição;
5. $v_5 \neq w_5$, $v_6 \neq w_6$ e $v_7 \neq w_7$, neste caso o erro está na quarta posição;
6. $v_5 \neq w_5$, neste caso o erro está na quinta posição;
7. $v_6 \neq w_6$, neste caso o erro está na sexta posição;
8. $v_7 \neq w_7$, neste caso o erro está na sétima posição.

Antes de mostrarmos este algoritmo em ação, entendemos que cabe aqui uma breve explicação, caso a caso, do por que do seu funcionamento.

1. No caso 1 não temos muito o que explicar, pois todos as verificações de paridade coincidem, logo, o simbolo enviado foi recebido sem erro.
2. No caso 2 ao notarmos que $v_5 \neq w_5$ e $v_6 \neq w_6$ concluímos que $v_7 = w_7$ e como $v_7 = d_2 + d_3 + d_4$ o erro não pode estar em d_2, d_3 ou d_4, logo, só pode estar em d_1, pois é a discrepancia de valores neste dígito que faz com que $v_5 \neq w_5$ e $v_6 \neq w_6$.
3. No caso 3 ao notarmos que $v_5 \neq w_5$ e $v_7 \neq w_7$, concluímos que $v_6 = w_6$ e como $v_6 = d_1 + d_3 + d_4$ o erro não pode estar em d_1, d_3 ou d_4, logo, só pode estar em d_2, pois é a discrepancia de valores neste dígito que faz com que $v_5 \neq w_5$ e $v_7 \neq w_7$.
4. No caso 4 ao notarmos que $v_6 \neq w_6$ e $v_7 \neq w_7$, concluímos que $v_5 = w_5$ e uma vez que $v_5 = d_1 + d_2 + d_4$ o erro não pode estar em d_1, d_2 ou d_4, logo só pode estar em d_3, pois é a discrepancia de valores neste dígito que faz com que $v_6 \neq w_6$ e $v_7 \neq w_7$.
5. No caso 5 ao notarmos que $v_5 \neq w_5$, $v_6 \neq w_6$ e $v_7 \neq w_7$, concluímos que o erro só pode estar em um dígito que é comum a v_5, v_6 e v_7, o qual como pode ser visto facilmente, é d_4, pois é a discrepancia de valores neste dígito que faz com que $v_5 \neq w_5, v_6 \neq w_6$ e $v_7 \neq w_7$.

6. Nos casos 6, 7 e 8 ao notarmos que $v_5 \neq w_5, v_6 \neq w_6$ e $v_7 \neq w_7$, respectivamente, tendo em vista as observações anteriores, só podemos conluir que o erro ocorreu na posição v_5, v_6 ou v_7, respectivamente.

Vejamos com um exemplo como este procedimento funciona na correção de um único erro de um símbolo.

Exemplo 2.52. Suponha que o símbolo $x' = 0101010$ tenha sido transmitido com um erro na quinta posição, ou seja, o símbolo recebido foi $x'' = 0101110$. Aplicando o Algoritmo 2.51 ao símbolo recebido, nós temos que $w_5 = d_1 + d_2 + d_4 = 0 + 1 + 1 = 0, w_6 = d_1 + d_3 + d_4 = 0 + 0 + 1 = 1$ e $w_7 = d_2 + d_3 + d_4 = 1 + 0 + 1 = 0$. Comparando com $v_5 = 1, v_6 = 1$ e $v_7 = 0$ fica fácil ver que $v_5 \neq w_5$, logo o erro está na quinta posição, como já era de se esperar. Para corrigir o erro, basta modificar o símbolo da quinta posição, trocando o 1 por um 0 e para decodificar o símbolo, basta tomar as 4 primeiras posições.

Com os Algoritmos 2.50 e 2.51 podemos codificar, decodificar e corrigir um único erro de qualquer um dos 16 símbolos do código $C(7,4)$. Entretanto, existe uma maneira mais prática de se codificar, decodificar e corrigir um único erro neste código, mais ainda, tal maneira é facilmente generalizada para a família de códigos $C(2^k-1, 2^k-k-1)$.

Considerando a Tabela 8 observamos que os coeficientes de $d_1, \cdots, v_7$ presentes em suas entradas são os mesmos da matriz,

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

a qual é chamada de *matriz geradora* do código $C(7,4)$, visto que qualquer símbolo W deste código é codificado no símbolo W' através da sua multiplicação com a matriz geradora, ou seja, $W' = WG_3$. O índice 3 designa o número de dígitos de verificação do código que, como já vimos anteriormente, neste caso são 3.

Exemplo 2.53. Para codificar o símbolo $x = 0101$ novamente, basta realizar a multiplicação das matrizes

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

e

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

obtendo a matriz

$$XG_3 = X' = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

a qual representa o símbolo codificado $x' = 0101010$. Note que obtemos o mesmo símbolo codificado que anteriormente.

Para o caso geral da matriz geradora de um código $C(2^k - 1, 2^k - k - 1)$, nós temos a seguinte definição;

Definição 2.54. A matriz geradora, denotada G_k, é uma matriz de dimensão $(2^k - k - 1) \times (2^k - 1)$ com coeficientes em $\mathbb{Z}_2$, tal que todos os elementos codificados do código C são obtidos através da sua multiplicação pela matriz geradora.

Outra matriz que possui destaque no código de Hamming é a chamada *matriz de controle* ou *matriz de paridade* H_k. Para o código $C(7, 4)$ temos que,

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

e para o caso geral, temos que a matriz de paridade de um código $C(2^k - 1, 2^k - k - 1)$ é definida como segue[24].

Definição 2.55. A matriz de paridade, denotada por H_k, é uma matriz de dimensão $k \times (2^k - 1)$ com coeficientes em $\mathbb{Z}_2$, tal que $G_k H_k^t = \mathbf{0}$, onde H_k^t denota a *matriz transposta* de H_k e $\mathbf{0}$ a matriz nula.

Note que as matrizes G_3 e H_3 do código $C(7, 4)$ podem ser escritas como $G_3 = [I_4 \ \ A]$ e $H_3 = [B \ \ I_3]$, em que A e B são matrizes satisfazendo $A^t = B$ e I_3 e I_4 denotam as

[24] O leitor com conhecimentos de Álgebra Linear deve ter percebido que as linhas da matriz geradora formam uma base para um espaço vetorial que é isomorfo a $\mathbb{Z}_2^{2^k-k-1}$. Mais ainda, nota-se também que as colunas da transposta da matriz de paridade formam uma base para o complemento ortogonal do espaço vetorial gerado pelas linhas da matriz geradora.

matrizes identidade de dimensão 3 e 4, respectivamente. Além disso, quando as matrizes G_3 e H_3 estão escritas nesta forma dizemos que as mesmas estão em sua *forma padrão*. A generalização deste fato é o conteúdo do próximo teorema, o qual nos permitirá obter G_k em sua forma padrão, sempre que definirmos H_k também em sua forma padrão e vice versa. A demonstração deste teorema não será inserida aqui, pois se utiliza de conceitos que fogem do escopo deste trabalho, porém a mesma pode ser encontrada em (MENEGHESSO, 2012, pp. 19 - 20).

Teorema 2.56. *Sejam $G_k = [I_{2^k-k-1} \ \ A]$ e $H_k = [B \ \ I_k]$. H_k será a matriz de verificação de paridade associada à matriz geradora G_k se, e somente se, $A^t = B$. Além disso, o código binário correspondente $C(2^k-1, 2^k-k-1)$ será corretor de um único erro se, e somente se, as colunas de H_k forem não nulas e distintas.*

Em vista do Teorema 2.56, uma pergunta que pode surgir é: "As matrizes G_k e H_k são as únicas que definem um código da forma $C(2^k-1, 2^k-k-1)$?". A resposta para esta pergunta é negativa e para verificarmos que de fato é, basta notarmos que a definição de códigos equivalentes (Definição 2.41) pode ser traduzida para o contexto das matrizes através da definição a seguir.

Definição 2.57. Duas matrizes G_k e G'_k geram o mesmo código C, ou seja, são equivalentes, se uma pode ser obtida da outra através de uma sequência finita de operações do tipo:

L1 Permutação de duas linhas;

L2 Adição de uma linha a outra;

C1 Permutação de duas colunas.

Exemplo 2.58. É fácil ver que a matriz geradora do código de Hamming definido na Seção 2.4 através do Algoritmo 2.15 é igual a

$$G_3 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

A qual, por sua vez é equivalente à matriz geradora do código de Hamming que definimos nesta seção à partir da Tabela 8

$$G'_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Pois podemos obter uma da outra através de aplicações sucessivas das operações acima definidas.

Para o caso geral, temos a seguinte proposição, cuja demonstração segue da simples aplicação das operações $(L1), (L2)$ e $(C1)$, para uma demonstração desta proposição para o caso onde o corpo em que as matrizes geradora e de paridade são definidas é um corpo K qualquer, ver (HEFEZ; VILLELA, 2008, pp. 92 - 93).

Proposição 2.59. *Dado um código C com matriz geradora G_k, existe um código equivalente C' com matriz geradora G'_k na forma padrão.*

Isto posto, temos que definida uma matriz geradora G_k, a codificação de um símbolo u qualquer do código $C(2^k - 1, 2^k - k - 1)$, se dá simplesmente pela multiplicação de u por G_k, obtendo-se o símbolo codificado $v = uG_k$, ou seja, a codificação é simplesmente uma multiplicação de matrizes com coeficientes em $\mathbb{Z}_2$. Para a decodificação e correção há dois casos: i) o símbolo foi transmitido sem erro; e ii) o símbolo foi transmitido com um único erro.

Para o primeiro caso, se o símbolo codificado v foi transmitido sem erro, então o mesmo é anulado pela matriz de paridade. Com efeito, $vH_k^t = (uG_k)H_k^t = u(G_kH_k^t) = u0 = 0$, assim, sempre que o produto vH_k^t for igual à matriz nula, podemos concluir que o símbolo foi transmitido sem erro.

Para o segundo caso, sejam v um símbolo do código $C(2^k - 1, 2^k - k - 1)$ (sem erro) e $v^{(i)} \in \mathbb{Z}_2^{2^k-1}$ o símbolo obtido pela adição, em $\mathbb{Z}_2$, de 1 ao i-ésimo dígito de v. Logo, $v^{(i)}$ é um símbolo codificado transmitido com um erro no i-ésimo dígito. Assim podemos escrever $v^{(i)} = v + (0 \cdots 0 \underbrace{1}_{i-\text{ésimo dígito}} 0 \cdots 0)$, donde segue que,

$$v^{(i)}H_k^t = \underbrace{vH_k^t}_{0} + \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} H_k^t = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} H_k^t.$$

Note que $v^{(i)}H_k^t$ é a i-ésima linha de H_k^t, logo, a i-ésima coluna de H_k. Dessa forma, um erro ocorrido na i-ésima posição da mensagem trasmitida equivale a i-ésima coluna de H_k, logo para corrigir o erro temos que modificar o dígito do símbolo recebido na posição que é equivalente a i-ésima coluna da matriz de paridade.

A seguir, ilustramos como esse procedimento funciona em dois exemplos, a correção de um símbolo do código $C(7,4)$ e para o código $C(15,11)$, os quais são os códigos para $k=3$ e 4 no código $C(2k-1, 2^k-k-1)$, respectivamente.

Exemplo 2.60. Vamos como corrigir um erro em um símbolo do código $C(7,4)$. Para isso, consideremos novamente o símbolo $x = 0101$, que como pôde ser visto no Exemplo 2.53 ao ser codificado, se torna $x' = 0101010$. Assim como fizemos no Exemplo 2.52, vamos introduzir um erro na quinta posição, obtendo $x'' = 0101110$. Para corrigir este erro, vamos multiplicar o símbolo x'' pela matriz de paridade para este código H_3, obtendo,

$$X''H_3^t = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix},$$

a quinta linha de H_3^t e consequentemente a quinta coluna de H_3, logo, o erro se encontra na quinta posição do símbolo x'' assim como já esperávamos.

Antes de irmos para o próximo exemplo, note que no código $C(15,11)$ os símbolos são escritos na forma $d_1d_2d_3\cdots d_{11}v_{12}v_{13}v_{14}v_{15}$, e que extendendo o Algoritmo 2.50 para este caso, podemos definir:

$$\begin{aligned} v_{12} &= d_1+d_2+d_4+d_5+d_7+d_9+d_{11} \\ v_{13} &= d_1+d_3+d_4+d_6+d_7+d_{10}+d_{11} \\ v_{14} &= d_2+d_3+d_4+d_8+d_9+d_{10}+d_{11} \\ v_{15} &= d_5+d_6+d_7+d_8+d_9+d_{10}+d_{11} \end{aligned} \tag{2.2}$$

Esta maneira de definir v_{12}, v_{13}, v_{14} e v_{15} é equivalente à definição de v_1, v_2, v_4 e v_8 dada pelo Algoritmo 2.15 na Seção 2.4, e a relação entre os dígitos lá e aqui pode ser vista na Tabela 9. Desta forma, para construir a matriz geradora $G_4 = [I_4 \ \ A]$, basta tomar $A = [v_{12}v_{13}v_{14}v_{15}]$, onde cada uma das quatro colunas de A é formada pelos coeficientes dos dígitos $d_i, i = 1\cdots 11$, que definem v_{12}, v_{13}, v_{14} e v_{15}.

Tabela 9 – Equivalência entre os digitos v_{12}, v_{13}, v_{14} e v_{15} e v_1, v_2, v_4 e v_8

Na Seção 2.4	v_1	v_2	d_3	v_4	d_5	d_6	d_7	v_8	d_9	d_{10}	d_{11}	d_{12}	d_{13}	d_{14}	d_{15}
Aqui	v_{12}	v_{13}	d_1	v_{14}	d_2	d_3	d_4	v_{15}	d_5	d_6	d_7	d_8	d_9	d_{10}	d_{11}

Fonte: O autor

Exemplo 2.61. O código $C(15, 11)$ codifica $2^{11} = 2048$ símbolos, a saber, $00000000000, \cdots,$ 11111111111 todas as sequências binárias contendo 11 elementos. Para a codificação, utilizamos a matriz geradora

$$G_4 = [I_{11} \;\; A] = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Pelo Teorema 2.56, a matriz de paridade é dada por

$$H_4 = [A^t \;\; I_4] = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Para codificar o símbolo $x = 10011100010$, realizamos a multiplicação da matriz

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

pela matriz G_4, obtendo a matriz

$$XG_4 = X' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

a qual representa o símbolo codificado $x' = 100111000101101$.

Suponha agora, que na transmissão de x' ocorreu um erro na 8ª posição, de sorte que o símbolo recebido tenha sido $x'' = 100111010101101$. Para corrigir este erro, multiplicamos a matriz

$$X'' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

pela transposta da matriz de paridade H_4^t, obtendo a matriz

$$X''H_4^t = \begin{pmatrix} 0 & 0 & 1 & 1 \end{pmatrix}$$

note que esta é justamente a a 8ª linha da matriz H_4^t, ou seja, a 8ª coluna de H_4, o que confirma que o erro se encontra no 8º dígito do símbolo recebido, como já era de se esperar.

.

Com este exemplo encerramos as considerações sobre o Código de Hamming e concluímos esse capítulo, tendo cumprido o segundo objetivo deste trabalho, elaborando uma apresentação do Código de Hamming utilizável por professores e alunos do Ensino Médio.

No Apêndice A, apresentamos um pequeno programa feito no Excel para obter os elementos do código do exemplo anterior, bem como corrigir um único erro. Este programa pode ser bastante útil na sequência didática facilitando o trabalho dos alunos quando forem trabalhar com este código, evitando assim cálculos que podem tornar as atividades cansativas e maçantes.

3 Sequência Didática

Neste capítulo, desenvolvemos uma proposta de sequência didática para o estudo dos códigos corretores de erros no Ensino Médio. Para isso, nas aulas que compõem a mesma, abordaremos alguns conceitos fundamentais na relação matemática-tecnologias digitais, os quais, servirão de contexto para a introdução dos códigos corretores de erros, bem como para mostrar como as tecnologias mais comuns do nosso cotidiano como, por exemplo, smartphones, computadores e internet, são profundamente dependentes de alguns conceitos matemáticos básicos, como é o caso do sistema binário de numeração.

Mais precisamente, nesta sequência didática abordaremos três temas principais, a saber:

i) a estrutura, o funcionamento e os componentes básicos de um computador;

ii) o sistema binário de numeração e o código ASCII - *American Standard Code for Information Interchange* (Código Padrão Americano para o Intercâmbio de Informações);

iii) códigos corretores de erros, mais especificamente, o código de Hamming, em suas duas formulações dadas no Capítulo 2.

Esta sequência didática será composta de 8 aulas com cada uma delas sendo organizada de modo que possa ser aplicada em uma turma do 2º ano, bem como em grupos de estudo compostos por alunos dos três anos do Ensino Médio. Cada aula tem a previsão de 50 minutos de duração (duração usual de uma aula na escola pública em Pernambuco), será composta segundo a estrutura no quadro abaixo e versará sobre conteúdos que ou foram abordados no Capítulo 2 deste texto ou estão presentes no Apêndice B. Vale lembrar também que caso tais aulas sejam dadas em uma escola pública com ensino médio regular, as mesmas cobrirão um período de cerca de duas semanas, e caso sejam dadas em uma escola de referência, cobrirão um período de cerca de uma semana e meia, visto que na primeira normalmente tem-se quatro aulas de matemática por semana, enquanto que na segunda, tem-se seis.

Quadro 1 - Estrutura das aulas

Justificativa: motivos pelos quais a aplicação das aulas deve ser realizada.
Objetivos: o que desejamos que os alunos compreendam através das aulas.
Recursos didáticos: materiais necessários para o bom funcionamento das aulas.
Conteúdos: o que será ensinado nas aulas.
Atividades: propostas geradoras de contexto para o desenvolvimento dos conteúdos a serem ensinados e/ou situações onde os conteúdos ensinados nas aulas são aprofundados.
Lista de exercícios: conjunto de exercícios que visam a consolidação e o aprofundamento dos conteúdos e atividades vistos nas aulas.
Avaliação: propostas e/ou instrumentos de avaliação para verificar as aprendizagens dos alunos após a aplicação das aulas.
Orientações ao professor: conjunto de informações e/ou leituras complementares, as quais podem ser consultadas pelo professor para um melhor aproveitamento das aulas da sequência didática.

3.1 1ª aula – Estrutura, funcionamento e componentes básicos de um computador

Justificativa: Aparentemente, todos nós, professores e alunos, sabemos o que é, para que serve e como funciona um computador, além disso, estranharíamos se conhecêssemos uma pessoa, que em pleno século XXI, não soubesse o que é esta máquina e nem para que ela serve. Porém, a dura realidade da escola pública em Pernambuco, é que embora os alunos saibam o que é um computador, estejam há muito tempo habituados com a sua presença em seu cotidiano, naveguem na internet com frequência e sejam visitantes assíduos de sites como YouTube, Facebook e Twitter, por exemplo, os mesmos nunca se perguntaram como é que esta máquina realmente funciona. Pior do que isso, é o fato de que são raros os casos daqueles que entraram em contato com ferramentas de programação e criação de aplicativos, o que em certa medida, está em última análise, os preparando para serem apenas usuários passivos destas tecnologias, contribuindo pouco ou nada para o seu desenvolvimento e utilização consciente.

Por este motivo, entendemos ser relevante antes de abordarmos os códigos corretores de erros, deixarmos bastante claro para os nossos alunos, onde e como estes são utilizados e acreditamos que o computador é um exemplo ideal para tal objetivo. Desse modo, a compreensão de como funciona um computador, ainda que de forma introdutória, pode despertar a curiosidade dos alunos para o papel dos códigos corretores de erros, como também para todo o universo da computação, o qual é uma das grandes fontes de pesquisas e desenvolvimentos tecnológicos tanto atualmente, quanto para as gerações futuras.

Vale destacar também que os princípios presentes na estrutura e funcionamento de um computador podem facilmente ser aplicados, com as devidas modificações, a outros artefatos tecnológicos como é o caso dos smartphones. Por isso, compreender estes elementos básicos podem abrir portas para outros avanços por parte dos alunos na direção de uma futura carreira na área das tecnologias digitais.

Objetivos: Os objetivos destas aulas são detalhar a estrutura, o funcionamento e os componentes básicos de um computador e apresentar os mesmos como o ambiente no qual os códigos corretores de erros encontraram suas primeiras aplicações e contextos para desenvolvimento.

Recursos didáticos: Data show, computador, quadro branco e pincel.

Conteúdos: Estrutura, funcionamento e componentes básicos de um computador. Um detalhamento destes conteúdos pode ser encontrado no Apêndice B.

Atividade: Não propomos atividades para estas primeiras aulas.

Lista de exercícios: Não propomos lista de exercícios para estas primeiras aulas.

Avaliação: Nesta aula não propomos atividades avaliativas, pois a mesma tem por objetivo iniciar as discussões sobre o assunto de forma simples, bem como apresentar um contexto no qual os códigos corretores de erros fazem sentido.

Orientações ao professor: Vale lembrar aqui, que um número incontável de alunos costumam perguntar aos seus professores de matemática para que serve a matemática que eles estão estudando. Em contrapartida, estes mesmos alunos não se dão conta de que todas as vezes que eles curtem uma foto ou um vídeo em suas redes sociais favoritas, digitam um texto para um trabalho escolar, assistem suas séries prediletas ou fazem uma simples pesquisa na internet, eles estão utilizando uma enorme quantidade de matemática, que embora nem sempre seja simples de ser compreendida, exerce um papel de extrema importância em suas vidas imersas na era digital.

Por este motivo, o professor deve procurar enfatizar o papel da matemática no projeto e funcionamento dos computadores, tarefa esta que pode ser em muito facilitada pelo auxílio de um bom material bibliográfico sobre o assunto. Para os interessados em estudar o tema de diferentes pontos de vista, indicamos as leituras de (ISSACSON, 2014), o qual estuda o surgimento e a evolução do computador à partir das biografias dos sujeitos envolvidos nesta tarefa, (STEWART, 1995, pp. 255 - 268), onde é possível encontrar uma apresentação clara e acessivel da relação entre o funcionamento de um computador e a forma binária de se representar os números, dentre outras coisas mais, e (RUDDER, 2015) que neste seu *bestseller* nos mostra como a vida na era digital tem moldado a forma como nos comportamos e nos relacionamos em sociedade.

Há também muitos vídeos que podem ser encontrados em algumas plataformas

digitais como, por exemplo, o YouTube[1], os quais podem ser utilizados pelos alunos como material de apoio aos estudos sobre a origem dos primeiros computadores, bem como sua estrutura e funcionamento. O professor interessado em realizar alguma avaliação do estudo realizado nestas aulas pode solicitar aos alunos que desenvolvam apresentações baseadas em vídeos como estes, e à partir daí, avaliar o que os seus alunos apreenderam sobre a origem dos computadores, bem como do seu papel e importância na sociedade atual.

3.2 2ª a 4ª aulas – O sistema binário de numeração e o código ASCII

Justificativa: O estudo e a compreensão correta dos números e das operações elementares na base 10 é um assunto recorrente em várias diretrizes e parâmetros curriculares para a Educação Básica, tanto em nível Nacional quanto em nível Estadual (BRASIL, 1997; BRASIL, 1998; BRASIL, 2000; BRASIL, 2002; PERNAMBUCO, 2012; PERNAMBUCO, 2013). Entretanto, dentre todos estes documentos, apenas em (PERNAMBUCO, 2013) encontramos breves recomendações para o professor trabalhar com outras bases numéricas que não a base 10 (p. 139), bem como para se utilizar do contexto dos computadores no ensino de questões relacionadas a grandezas e medidas (p. 161). Tendo isso em vista, entendemos ser relevante apresentar aos alunos outras bases numéricas, em particular a base 2, como também os contextos onde a mesma pode ser encontrada, além de alguns problemas interessantes relacionados a esta forma particular de se representar os números.

A compreensão de como funciona o sistema binário de numeração é um dos primeiros passos para o bom entendimento de toda a ciência relacionada com o funcionamento e o desenvolvimento de computadores. Vale ressaltar também que um dos elementos mais básicos neste sentido é o código ASCII[2] (ver Tabela 1), o qual é exemplo de uma das mais importantes aplicações do sistema binário de numeração na computação. Tal fato, nos leva a crer que a introdução e o estudo do mesmo na Educação Básica, pode consistir em mais um elemento contribuindo no desenvolvimento de uma prática da matemática escolar mais próxima das demandas da sociedade atual. Tudo isso acarreta uma maior compreensão, partindo dos novos profissionais que saem da escola para o mercado de trabalho, de como o mundo digital funciona em seus níveis mais técnicos, o que visto em perspectiva, significa

[1] Para alguns vídeos versando sobre a origem e funcionamento do computador, ver: <https://www.youtube.com/watch?v=QrFIvig2Kns>, <https://www.youtube.com/watch?v=jH5gOJvvCSQ> e <https://www.youtube.com/watch?v=wyZPsCQd7Uo>. Para uma curiosidade sobre a origem dos smartphones, ver <https://www.youtube.com/watch?v=jPsqInAxm6w>, e para uma discussão mais voltada para o papel que as tecnologias exercerão no futuro, ver: <https://www.youtube.com/watch?v=OEo14_iw7ho>

[2] O código ASCCI foi desenvolvido tendo em vistas a facilitação e universalização da programação de computadores, o que contribuiu bastante para que os computadores viessem a ter a importância que tem atualmente. Para maiores detalhes sobre a criação do código ASCII, acessar o site: <http://cultura.ufpa.br/dicas/progra/arq-asc.htm>

profissionais que não são apenas usuários das tecnologias digitais mas, mais do que isso, são usuários críticos e possíveis desenvolvedores das mesmas.

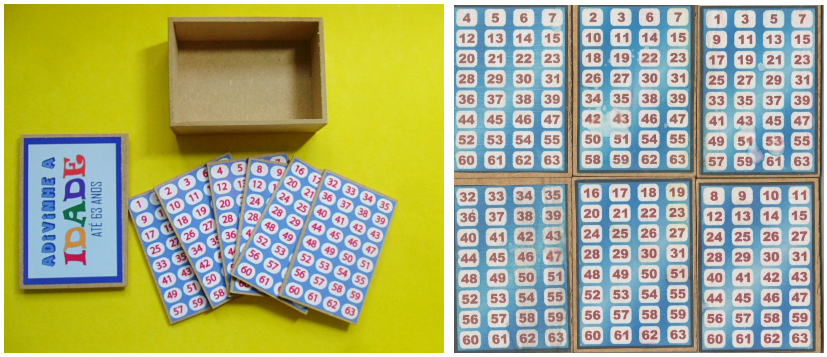
Objetivos: Os objetivos destas aulas são apresentar o sistema binário de numeração como mais uma alternativa para a representação dos números e apresentar o código ASCII como uma ferramenta que se utiliza desta forma particular de se representar os números, para desenvolver todo um campo da ciência.

Recursos didáticos: Jogo "Adivinhe a idade", Data show, computador, calculadora de smartphone, quadro branco e pincel.

Conteúdos: Sistema de numeração binário e código ASCII.

Atividade 1 (Descobrindo a idade): Um dos truques matemáticos mais difundidos entre os professores, alunos e interessados em recreações matemáticas é o que, através de uma série de passos ou instruções, permite ao aplicador do truque descobrir a idade de uma pessoa. Dentre os inúmeros truques existentes, decidimos apresentar nesta atividade o truque chamado "Adivinhe a idade", pois com o mesmo é possível trabalhar a representação de um número na base 10 se utilizando apenas de potências de 2.

Figura 15 – Cartões "Adivinhe a idade"



Fonte: Google Images

O truque é feito da seguinte maneira: o aplicador do truque mostra para a pessoa a quem o truque está sendo feito os cartões da Figura 15 e pede para a mesma dizer em quais cartões aparecem a sua idade, em seguida, o aplicador do truque supreende a seu interlocutor dizendo qual é a sua idade.

O aplicador consegue "descobrir a idade" da pessoa, simplesmente somando os números que aparecem na primeira posição da primeira linha de cada cartão. Por exemplo, se digo que minha idade está presente nos cartões que começam com $4, 8$ e 16, então o aplicador pode concluir rapidamente, que minha idade é $4 + 8 + 16 = 28$ anos. Note porém, que este truque só funciona para idades entre 1 e 63 anos e caso queiramos ampliar as idades a serem descobertas, devemos também aumentar a quantidade de cartões, por exemplo, para idades de 1 à 127 anos são necessários 7 cartões.

Nesta atividade o professor formará grupos de 4 ou 5 alunos e explica para apenas um deles como o jogo funciona. Em seguida, pode escolher entregar o jogo já pronto para os alunos e deixar que eles o explorem ou antes disso, reservar um tempo para que os próprios alunos construam o jogo. De qualquer forma, permitir que os alunos explorem o funcionamento do jogo e busquem uma solução para o seu funcionamento será benéfico para que, além de desenvolverem suas habilidades matemáticas de reconhecimento de padrões, por exemplo, os mesmos se envolvam com a atividade proposta, tornando-a assim mais significativa.

Atividade 2 (a multiplicação egípcia): A forma como os antigos egípcios efetuavam as suas multiplicações é particularmente curiosa, devido ao fato deles implicitamente se utilizarem da representação de um número como a soma de potências de 2, assim como ocorre no truque anterior. Vejamos um exemplo, baseado em (ROQUE, 2012, p. 79).

Quando um escriba egípcio queria multiplicar, por exemplo, 12 por 27 ele formava duas colunas de números, na primeira ele colocava todas potências de 2 menores do que 27 e na segunda, ele começava pelo 12 e os números seguintes eram obtidos simplesmente dobrando o valor do número que o precedia. Feito isso, o escriba escolhia na primeira coluna os números cuja soma dava 27 (ele fazia isso, os marcando com uma barra), ou seja, os números escolhidos seriam $1, 2, 8$ e 16, os números na segunda coluna associados a estas potências de 2 são $12, 24, 96$ e 192, respectivamente, cuja soma é $12 + 24 + 96 + 192 = 324$, ou seja, o resultado da multiplicação de 12 por 27.

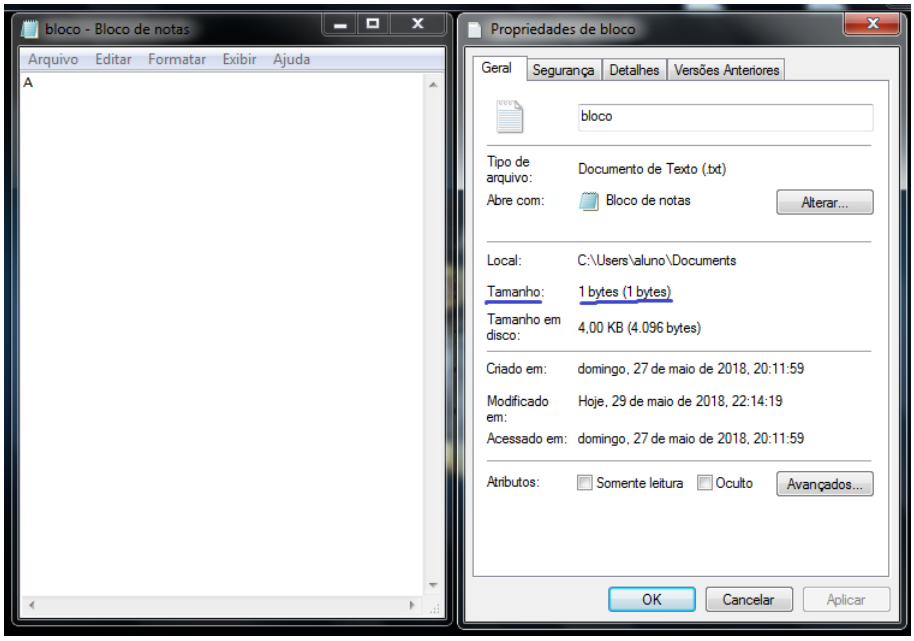
\	1	12
\	2	24
	4	48
\	8	96
\	16	192
$Total:$	27	324

Nesta atividade o professor pode incentivar os alunos a resolverem algumas multiplicações utilizando este método, e consequentemente realizarem uma comparação deste método com o método de multiplicação que utilizamos usualmente, verificando assim, se há alguma semelhança entre os mesmos, bem como, em que situações um é mais prático do que o outro.

Atividade 3 (Medindo a informação): Nesta atividade veremos como a definição do bit dada por Shannon em 1948, permitiu que posteriormente a informação pudesse ser quantificada como a conhecemos hoje, em termos de megabytes, gigabytes e etc.

Abra em seu computador um arquivo no formato bloco de notas e escreva apenas uma letra, em seguida, salve o arquivo com um nome qualquer e verifique qual o tamanho do arquivo.

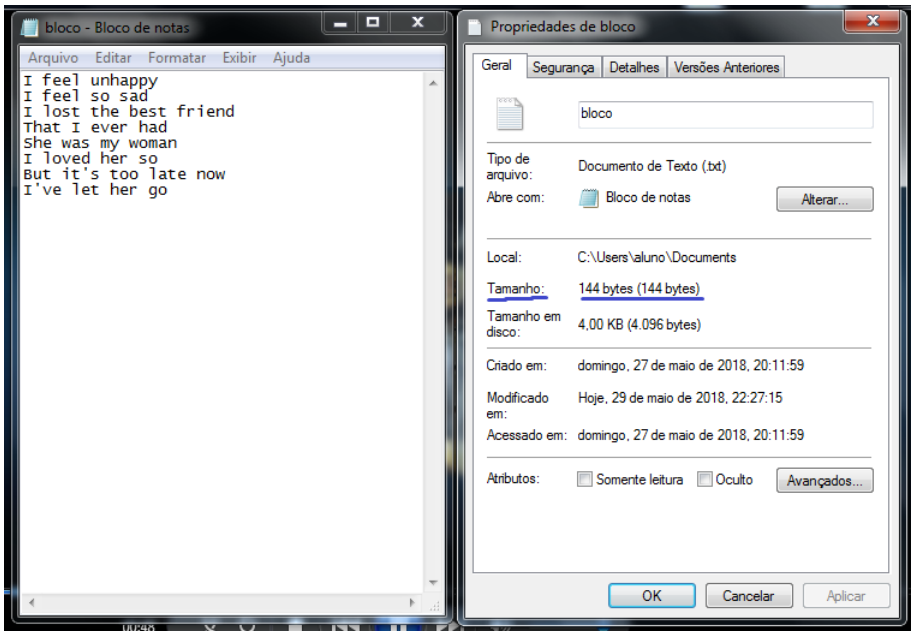
Figura 16 – Tamanho de um arquivo com uma letra.



Fonte: O autor

Para verificar o tamanho do arquivo, clique com o botão esquerdo do mouse sobre o arquivo e escolha a opção *propriedades*, tal comando vai gerar a janela da imagem à esquerda da Figura 16.

Figura 17 – Tamanho de um arquivo com trecho de música.



Fonte: O autor

Lá podemos ver claramente que o tamanho do arquivo é de 1 byte, pois escrevemos

apenas uma letra, a qual no código ASCII é definida por uma sequencia de 8 bites, ou seja 1 byte. Por outro lado, na Figura 17, temos o tamanho do arquivo contendo o trecho de uma música[3],note que o tamanho do arquivo é 144 bytes, porém o trecho só possui 130 caracteres, contabilizando 130 bytes. Os 14 bytes excedentes se devem às 7 linhas novas, além da primeira linha, cada uma correspondendo a 2 bytes.

Lista de exercícios

1. Utilizando o método egípcio de multiplicação realize os seguintes produtos: $12 \times 89, 198 \times 128, 61 \times 367$ e 157×1016.

2. Some os pares de números $(1000011)_2$ e $(1100111)_2$, $(00111010)_2$ e $(11001010)_2$ e $(1111000100)_2$ e $(1110000010)_2$. (Dica: a soma de números em sua forma binária se faz de modo semelhante à sua forma decimal, a diferença é que no caso da base 10 a cada vez que somamos 10 o algarismo se 'desloca uma casa' para a esquerda, enquanto que no caso da base 2 isso ocorre a cada vez que somamos 2).

3. Multiplique os pares de números da questão anterior. (Dica: a ideia aqui é a mesma da soma. Para verificar seus cálculos faça a mesma conta na base 10 e confira se o seu resultado obtido na base 2 confere com o da base 10).

4. Escreva os números $(1010110)_2, (010110011)_2, (100001)_2, (1010011010)_2$ e $(11111000101)_2$ em sua representação decimal.

5. Escreva os números $37, 83, 109, 269$ e 1087 como a soma de potências de 2.

6. Escreva os números da questão anterior em sua representação binária.

7. Utilizando o código ASCII da Tabela 1 escreva como uma sequência binária a frase: *It's a trap.*

8. Utilizando o código ASCII da Tabela 1 decodifique a seguinte mensagem: 10100101 10110010 10110010 10101111 10110011 01000000 10110000 10101111 10100100 10100101 10101101 01000000 10110011 10100101 10110010 01000000 10100011 10101111 10110010 10110010 10101001 10100111 10101001 10100100 10101111 10110011.

9. Mostre que dado um peso de valor inteiro P, tal que $P \leq 63$ é possível o pesá-lo em uma balança de pratos utilizando seis pesos de valores $1, 2, 4, 8, 16$ e 32 quilos, respectivamente.

10. Mostre por que o truque "Adivinhe a idade" funciona. Mostre também que para adivinhar idades entre 1 e $2^i - 1$ anos, com i inteiro positivo, são necessários i cartões. (Dica: Corolário 2.21).

[3] Changes, 3ª música do 4º albúm da banda britânica de heavy metal Black Sabbath, lançado em 1972.

11. Mostre por que o método de multiplicação egípcio funciona. (Dica: Use o Corolário 2.21).

12. Estenda o método egípcio para a realização de divisões. (Dica: Consulte a referência (ROQUE, 2012, p. 79).)

Avaliação: Estas aulas introduzem vários elementos ricos em situações que podem ser utilizadas para compor uma avaliação dos alunos. Como proposta de avaliação destas aulas, sugerimos, além da lista de exercícios, o instrumento de avaliação *Mapas Conceituais com Vídeos*, o qual desenvolvemos em um estudo anterior, na ocasião do nosso trabalho de conclusão do curso de graduação em Licenciatura em Matemática. Para maiores detalhes sobre o que são mapas conceituais e como a utilização de vídeos na explicação dos mesmos torna este par mapas conceituais-vídeos um instrumento de avaliação, ver (LIRA, 2015).

Dessa forma, a avaliação aqui pode ser vista como atuando em duas frentes distintas, uma que visa compreender o quanto o aluno aprendeu do ponto de vista técnico e computacional (a lista de exercícios) e a outra que visa compreender o quanto o aluno está ciente dos conceitos envolvidos nas aulas estudadas, bem como a maneira que eles se relacionam entre si (os mapas conceituais com vídeos).

Orientações ao professor: O professor pode utilizar a Atividade 1 para consolidar o aprendizado dos alunos no que diz respeito à relação entre escrita de um número na base 10 e a sua respectiva escrita na base 2, há aqui também uma oportunidade de se explorar com maiores detalhes os conteúdos do Teorema 2.19 e do Corolário 2.21.

A Atividade 2 pode ser utilizada juntamente com uma abordagem do sistema binário de numeração, via história da matemática, a qual pode se mostrar uma alternativa para apresentar o mesmo de uma forma mais natural e intuitiva. Para isso, aconselha-se discorrer um pouco sobre como a multiplicação efetuada pelos antigos egípcios tem seu fundamento no sistema de numeração binário.

Outra opção é a leitura com os alunos do texto do matemático alemão Gottfried Wilhelm von Leibniz publicado em 1703 na revista *Mémoires de l'Académie des Sciences*, intitulado *Explication de l'arithmétique binaire*[4], no qual pela primeira vez na história o sistema de numeração binário é formalizado e apresentado ao mundo.

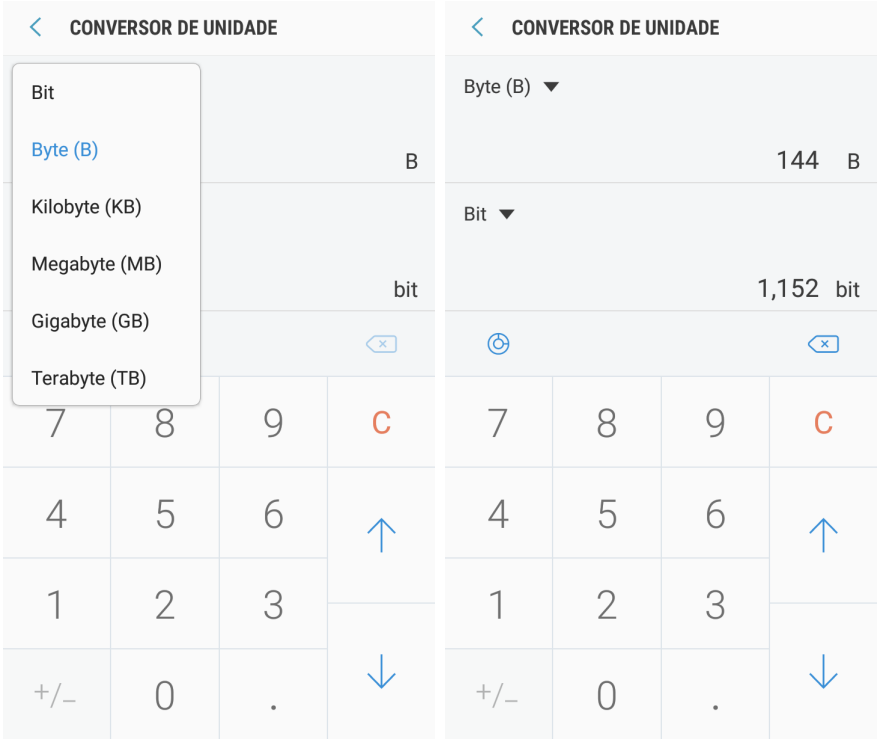
O professor também pode se utilizar mais uma vez do conhecimento da história da matemática, em particular, do contido em trabalhos clássicos como, por exemplo, (IFRAH, 2005, pp. 52 - 78) e (EVES, 2011, pp. 25 - 51), para apresentar o surgimento de diferentes

[4] Explication de l'arithmétique binaire, qui se sert des seuls caractères 0 et 1, avec des remarques sur son utilité, et sur ce qu'elle donne le sens des anciennes figures Chinoises de Fohi . Para uma tradução deste texto para o português ver: LOPES, F. J. A. Leibniz e a Aritmética Binária. Revista Brasileira de História da Matemática, Vol. 11 nº 22 (outubro/2011 - março/2012) - pp. 89 - 94. Disponível em:<http://www.rbhm.org.br/issues/RBHM%20-%20vol.11,no22/5%20-%20Fred.pdf>

bases numéricas, em diferentes povos e regiões do globo, como algo natural e intimamente relacionado com o corpo humano. Por exemplo, na contagem através de agrupamentos em 10 e 10 ou 20 em 20, que faziam referência direta com o número de dedos das mãos e das mãos e pés juntos, respectivamente. Para um trabalho mais direcionado, baseado em uma pesquisa feita diretamente na sala de aula, ver (MELO, 2017).

Cabe aqui lembrar o professor que a Atividade 3 pode ser um ambiente fértil para a utilização do celular como uma ferramenta útil no estudo da matemática. Como um exemplo o professor pode utilizar a calculadora do celular para facilitar conversões de unidades de medida de informação. Na Figura 18 temos um exemplo de uma destas calculadoras[5] em sua tela inicial (imagem da esquerda) e ao calcularmos a quantidade de bits que compreendem o arquivo de 144 bytes do trecho da música (imagem da direita.).

Figura 18 – Tamanho de um arquivo com trecho de música.



Fonte: O autor

Por fim, vale lembrar que um possível questionamento que será feito pelos alunos é sobre porque utilizar a forma binária de representar um número, quando em muitos casos como, por exemplo, no caso do número $(1000011)_2$ a forma binária parece ser mais

[5] A calculadora desta figura é a padrão de um smartphone (particularmente o do autor), porém aplicativos com funções semelhantes à função da calculadora mostrada são encontrados facilmente em plataformas digitais como, por exemplo, a Play Store. Também é fácil encontrar este tipo de calculadora na internet, para o exemplo de um site, ver <https://www.google.com.br/search?q=calculadora+de+convers%C3%A3o+de+dados&oq=calculadora+de+convers%C3%A3o+de+dados&aqs=chrome..69i57.9560j0j9&sourceid=chrome&ie=UTF-8>.

complicada que a forma decimal $(67)_{10}$. A resposta para este tipo de questionamento está intimamente relacionada com o funcionamento do computador visto na Aula 1, bem como na explicação dada por (STEWART, 1995, pp. 255 - 268), para a relação entre a escrita binária e o funcionamento da máquina.

3.3 5ª a 8ª aulas – Explorando o Código de Hamming

Justificativa: No Capítulo 1 desta dissertação, mostramos como os códigos corretores de erros têm passado por um processo de transposição didática, o qual embora ainda esteja em seus primeiros passos, já se mostra como uma possível tendência para o ensino futuro da matemática. Vale destacar que, conforme aponta (CAVALCANTI, 2010, pp. 3 - 4), uma tendência na educação matemática surge "[...] das pesquisas sobre as práticas realizadas em sala de aula, mas também de pesquisas realizadas fora da sala de aula.".

Dessa forma, entendemos que a concepção destas aulas, e no geral, desta dissertação, está de acordo com o que foi apontado como o surgimento de uma tendência em educação matemática, pois tal pesquisa aqui desenvolvida possui uma natureza teórica, bem como um ramo prático, aplicado diretamente na sala de aula, o que juntamente com os outros trabalhos desenvolvidos nesta mesma direção, fortalece a percepção de que estamos diante de uma possível tendência em educação matemática, quando falamos de códigos corretores de erros.

Além disso, vivemos em uma sociedade, conhecida como pós-moderna, que a cada dia depende mais e mais de artefatos tecnológicos os quais, por sua vez, dependem de um tipo de matemática muito diferente do ensinado nas escolas. Se por um lado, a matemática ensinada nos séculos XVII, XIX e início do XX tinha por um dos seus objetivos levar os alunos a compreenderem o funcionamento de artefatos mecânicos como, por exemplo, uma máquina de uma fábrica, por outro lado, a matemática da segunda metade do século XX e do século XXI, pode ser utilizada para ensinar e explorar o funcionamento de artefatos ícones da revolução digital, como é o caso dos smatphones e computadores, acompanhando assim, os avanços tecnológicos presentes na sociedade e no cotidiano dos alunos.

Objetivos: O objetivo destas aulas é identificar sistemas de comunicação nas mais variadas situações do cotidiano e estudar o código de Hamming tanto do ponto de vista do trabalho original de Hamming (HAMMING, 1950), quanto da sua formulação atual (ROUSSEAU; AUBIN, 2015).

Recursos didáticos: Computador, Data show, quadro branco e pincel.

Conteúdos: O código de Hamming.

Atividade 1 (Códigos detectores de um erro): Para esta atividade, a turma será decomposta em grupos de três alunos e irá simular um sistema de comunicação,

conforme definido no Capítulo 2. A função de cada aluno no grupo se dará da seguinte forma: o primeiro aluno fará o papel da *fonte de informação* e de *transmissor*, o segundo fará o papel de *fonte de erro*, e o último fará o papel de *receptor* e *destinatário*. O primeiro aluno vai escolher um símbolo do código ASCII (Tabela 1), por exemplo, 10101101 e codificá-lo utilizando o Algoritmo 2.11, gerando o símbolo 101011011. Em seguida, o segundo aluno terá a opção de introduzir ou não um erro em uma posição que ele escolher do símbolo codificado, digamos que ele decide trocar o 0 por 1 na 4ª posição, de forma que o símbolo 101111011 sejá transmitido para o terceiro aluno. Por fim, este aluno terá a tarefa de verificar se no símbolo existe ou não um erro.

Atividade 2 (Códigos corretores de um erro): Nesta atividade teremos a mesma configuração da turma utilizada na Atividade 1, e além de codificar um erro vamos corrigí-lo. O primeiro aluno vai escolher um símbolo do código ASCII, por exemplo, 10101101 e codificá-lo utilizando a Tabela 3 e o Algoritmo 2.15, gerando o símbolo 001001011101. Em seguida, o segundo aluno terá a opção de introduzir ou não um erro em uma posição que ele escolher do símbolo codificado, digamos que ele decide novamente trocar o 0 por 1 na 4ª posição, de forma que o símbolo 001101011101 sejá transmitido para o terceiro aluno. Por fim, este aluno terá a tarefa de decodificar o símbolo utilizando o Algoritmo 2.16, verificar se existe ou não um erro e caso exista, corrigí-lo.

Atividade 3 (Corrigindo erros com o Excel): Nesta atividade construímos no Programa Excel o código de Hamming $C(15, 11)$, Exemplo 2.61. Definiremos as matrizes geradora G_4 e de paridade H_4, bem como o processo de codificação e correção de um erro, através de algumas funções disponíveis no Excel, este processo será detalhado no Apêndice A.

Lista de exercícios

1. Utilizando o Algoritmo 2.11 para detecção de um erro, determine quais dos símbolos $10001101, 01100010, 01101001$, 00001110 e 11000110 do código $C(8, 7)$ possuem erro e quais foram transmitidos corretamente.

2. Um código tem símbolos que transmitem 8 bits de informação e são codificados em sequências de 12 bits. Qual é a redundância deste código? Se quisermos uma redundância 10% menor, qual deve ser o tamanho mínimo das sequencias dos símbolos codificados?

3. Utilizando a Tabela 3 e o Algoritmo 2.15 codifique os símbolos $0110, 1101, 1000, 0110$ e 1011 para os casos $k = 3$ e $k = 4$. No primeiro caso, temos o código $C(7, 4)$ e no segundo, o código $C(8, 4)$. Qual dos dois é o mais eficiente?

4. Utilizando o Algoritmo 2.16, decida se houve erro na transmissão dos símbolos $0110011, 0100001, 1110001, 0010010$ e 0110000.

5. Adaptado de (ROUSSEAU; AUBIN, 2015, p. 215) - a) No código de Hamming $C(7,4)$, quais são os símbolos a serem enviados se queremos transmitir os símbolos $0000, 0010, 0111$ e 1110?

   b) O receptor recebeu os símbolos $1111111, 1011111, 0000111$ e 1111000. Quais foram os símbolos transmitidos originalmente?

6. Adaptado de (ROUSSEAU; AUBIN, 2015, p. 215) - a) Se a matriz de paridade do código $C(15,11)$ é

$$H_4 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

   determine a matriz geradora G_4 e verifique que $G_4 H_4^t = 0$.

   b) Utilizando a matriz G_4 do item anterior, codifique os símbolos 00111111001, 11110010100 e 10000101110.

   c) Determine se houve erro de transmissão no símbolo 101010101010101. Caso houve, detemine onde e o corrija.

   d) Decodifique o símbolo do item anterior.

7. a) Se a matriz de paridade do código $C(7,4)$ é

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

   determine a matriz geradora G_3 e verifique que $G_3 H_3^t = 0$.

   b) Encontre a matriz G_3' escrita na forma padrão $[I_4 \;\; A]$ e equivalente a G_3.

   c) Determine se houve erro de transmissão no símbolo 1010011. Caso houve, determine onde e o corrija.

   d) Decodifique o símbolo corrigido no item anterior.

Avaliação: A avaliação destas aulas pode ser feita em dois momentos. No primeiro momento, o professor pode utilizar as Atividades 1 e 2 como instrumento de avaliação e no segundo momento, ele pode utilizar a lista de exercícios proposta anteriormente. Além disso, outra opção para o professor seria levar os alunos a utilizar o programa desenvolvido na Atividade 3 em situações semelhantes a proposta na Atividade 2 na transmissão de mensagens mais longas e complexas do que as que são possíveis com o código $C(7,4)$.

Orientações ao professor: Para que o conceito de um código corretor de erros fique bem definido e por sua vez, possa ser bem compreendido pelos alunos, três elementos

devem ser devidamente esclarecidos pelo professor, quais sejam, *codificação, correção* e *decodificação*. Não é possível se falar em um código corretor de erros sem que estes elementos estejam presentes, por isso, as diferentes formas de se realizar estes três procedimentos devem ser amplamente explicadas.

Um ponto que merece ser destacado com os alunos é o fato de o código de Hamming apresentado nestas aulas não ser o único código detector de erros existente, muito pelo contrário, é uma atividade interessante mostrar para os alunos códigos como o UPC - *Universal Product Code* e o EAN - 13 - *European Article Number* utilizados em códigos de barras, o ISBN - *International Standard Book Number* utilizado na catalogação de livros, bem como os números de RG, CPF e cartões de crédito, os quais se fazem presentes no cotidiano de muitos dos nossos alunos, são detectores de erros assim como o código de Hamming. Para um estudo sobre estes códigos ver (SÁ; ROCHA, 2012; MENEGHESSO, 2012) ou os exercícios 9, 10 e 11 de (ROUSSEAU; AUBIN, 2015, pp. 217 - 218).

Com a Atividade 1 o professor terá a oportunidade de trabalhar com os alunos o alcance do Algoritmo 2.11 verificando, por exemplo, que caso ocorra mais do que um erro, o mesmo pode passar despercebido no sistema, mais ainda, um número par de erros sempre passará despercebido, pois, isso conserva a quantidade par de números 1 no símbolo o que faz o receptor concluir errôneamente, que não ocorreram erros.

Com as Atividades 2 e 3 o professor terá a oportunidade de trabalhar com os alunos os Algoritmos 2.15 e 2.16 e após isso, discutir com os mesmos, como as contas começam a se tornar cada vez maiores, daí a necessidade da utilização de ferramentas mais adequadas - neste caso o auxílio da planilha Excel - para a realização dos cálculos com matrizes.

Concluímos aqui nossa proposta de elaborar uma sequência didática para o ensino do código de Hamming no Ensino Médio alcançado, o terceiro objetivo desta dissertação.

Encerramos o trabalho fazendo as considerações finais a seguir.

—

Considerações Finais

Nossa primeira intenção ao decidirmos abordar o tema Códigos Corretores de Erros no Ensino Médio, foi realizar um estudo sobre o desenvolvimento histórico dos mesmos, porém, ao nos debruçarmos sobre esta temática percebemos que tal estudo demandaria o aprofundamento de temas que não dominávamos no que diz respeito à historiografia e até mesmo a questões referentes ao contexto histórico da época que foi muito rico e complexo. Consequentemente exigiria um maior investimento do já escasso tempo que dispúnhamos para o estudo, na nossa condição de professor da Educação Básica. Decidimos então realizar um estudo com foco na matemática do Código de Hamming e sua utilização em sala de aula, pois abarcava o tema dos códigos corretores, que nos interessava, e se coadunava com nosso perfil acadêmico, nos deixando mais confortáveis diante da elaboração de um trabalho de finalização de mestrado.

Entendemos que uma pesquisa de natureza acadêmica não se encerra com sua escrita, uma vez que, naturalmente trás novas questões através de sua construção. Em nossa pesquisa, obtivemos alguns desdobramentos que pretendemos explorar futuramente, dentre os quais vislumbramos os seguintes:

1. Realizar um estudo detalhado das dissertações, já citadas na nota nº 1 do Capítulo 1, pois, acreditamos que o estudo de tais trabalhos pode reforçar a ideia levantada no Capítulo 1 de que o tema, *Códigos Corretores de Erros no Ensino Médio*, representa uma verdadeira tendência para o ensino de matemática das próximas gerações. Mais ainda, o processo de realização deste trabalho nos deixou com a impressão de que muito da matemática que foi desenvolvida na segunda metade do século XX, apresenta reais possibilidade, e até mesmo, grandes potencialidades de ser introduzida e abordada nos currículos de matemática de um futuro próximo, devido a sua íntima relação com as aplicações em tecnologias digitais e ao papel de destaque que computadores e celulares podem ter no ensino da matemática.

2. Aprofundar o estudo do rico e peculiar contexto histórico relacionado com os Códigos Corretores de Erros, buscando assim, elementos que possam ser aliados do professor na hora de ensinar os mesmos de uma forma mais contextualizada e natural.

3. Aplicar a sequência didática desenvolvida no Capítulo 3 em turmas do Ensino Médio, com vistas a identificar as potencialidades e limitações da proposta aqui empreendida, bem como para, a partir daí, fazer as modificações e adaptações necessárias para o seu melhor funcionamento diante das reais condições encontradas na sala de aula.

Reafirmamos aqui o que vimos destacando ao final de cada capítulo, que cada um dos três objetivos a que nos propusemos neste trabalho foram atingidos. Contudo, entendemos que cada um daqueles objetivos, quando aliados aos pontos que levantamos acima, evocam novas propostas de trabalho e caminhos de pesquisa que podemos percorrer, tendo em vista aprofundar o conhecimento sobre o tema, bem como, tornar mais clara e acessível nossa proposta de introdução dos Códigos Corretores de Erros no Ensino Médio. Assim, podemos destacar as seguintes implicações:

1. Do objetivo 1, pode advir um trabalho de mapeamento das pesquisas voltadas para a temática *Códigos Corretores de Erros no Ensino Médio*.

2. Do objetivo 2, entendemos que um estudo aprofundado do desenvolvimento histórico do tema pode contribuir na elaboração de propostas mais adequadas a este nível de ensino, bem como uma maior compreensão do papel da matemática na revolução digital e da construção da sociedade da informação, na qual estamos inseridos.

3. Do objetivo 3, podem advir materiais didáticos mais adequados a realidade vivenciada na sala de aula.

Por fim, gostaríamos de encerrar a nossa contribuição fazendo menção à epígrafe que iniciou esta dissertação: "*Tudo o que um homem imaginar, outros homens poderão fazer*". Esta frase, atribuída ao famoso escritor francês do século XIX Júlio Verne, nos mostra o quanto a nossa capacidade de imaginação é poderosa para mudar a realidade em que nos encontramos, fazendo com que coisas que na cabeça de alguns eram apenas imaginação se tornem realidades nas mãos de outros. Quando olhamos para o contexto da educação nacional e, em especial, da educação pernambucana, esta frase se revela particularmente significativa, bem como lança uma nova luz sobre a copreensão do nosso papel como estudante, pesquisador e professor na sociedade atual.

Um trabalho como este pode se mostrar, a princípio, apenas como a imaginação de um homem em ação. Apenas como um sonho otimista de que algum dia seremos capazes de ter uma escola pública e de qualidade alinhada com o seu tempo e capaz de preparar os jovens para o futuro que a cada dia se mostra mais presente. Um sonho de que os desafios do Ensino Médio no futuro não sejam os de lidar com alunos que não dominam as operações matemáticas básicas, mas sim o de trazer para esse jovem conteúdos significativos plenos de sentido como o estudado nesta dissertação. O sonho de que o professor tenha o seu trabalho reconhecido e que o seu papel na sociedade seja realmente valorizado e considerado na mais alta estima.

Enquanto não vemos este sonho tornado realidade em toda a nossa sociedade, continuamos estudando, pesquisando e ensinando matmática, na certeza de que um dia, o

sonho sonhado por muitos (dentre os quais se inclui o autor), será tornado em realidade por outros.

Referências

ABRANTES, S. A. *Notas históricas da codificação para controlo de erros.* 2003. Disponível em: <{https://paginas.fe.up.pt/~sam/textos/Notas%20hist%F3ricas.pdf}.>

AGUIAR, J. C. O.; VIEIRA, S. R.; CAVALCANTE, R. G. *Códigos Quânticos Corretores de Erros.* 2010. Disponível em: <{http://congressos.ifal.edu.br/index.php/connepi/CONNEPI2010/paper/viewFile/971/71}.>

ALVES, B. C. Mestrado Profissional em Matemática, *Uma Proposta de Oficina sobre Códigos para a Contextualização do Estudo de Aritmética e Matrizes no Ensino Médio.* Goiânia: [s.n.], 2015. 74 p.

AVILA, G. *Várias faces da matemática: tópicos para licenciatura e leitura geral.* 2. ed. São Paulo: Blucher, 2010. 203 p.

BLAINEY, G. *Uma breve história do século XX.* 2. ed. [S.l.]: Editora Fundamento Educacional, 2011. 307 p.

BOLLAUF, M. F. Mestrado em Matemática Aplicada, *Códigos, reticulados e aplicações em criptografia.* Campinas: [s.n.], 2015. 88 p.

BRASIL. *Parâmetros Curriculares Nacionais: Matemática.* Brasília: MEC/SEF, 1997. 142 p.

BRASIL. *Parâmetros Curriculares Nacionais: Matemática.* Brasília: MEC/SEF, 1998. 148 p.

BRASIL. *Parâmetros Curriculares Nacionais: Matemática.* Brasília: MEC/SEMTEC, 2000. 109 p.

BRASIL. *Diretrizes Curriculares Nacionais para os Cursos de Matemática, Bacharelado e Licenciatura. PARECER Nº: CNE/CES1.302/2001.* 2001. Disponível em: <{http://portal.mec.gov.br/cne/arquivos/pdf/CES13022.pd}.>

BRASIL. *PCN+Ensino Médio: Orientações Educacionais complementares aos Parâmetros Curriculares Nacionais.* Brasília: MEC/SEMTEC, 2002. 144 p.

CARROCINO, C. H. G. Mestrado Profissional em Matemática, *Questões contextualizadas nas provas de matemática.* Rio de Janeiro: [s.n.], 2014. 69 p.

CARVALHO, S. M. G. Mestrado Profissional em Matemática, *Matrizes, determinantes e polinômios: uma aplicação em códigos corretores de erros, como estratégia motivacional para o ensino de matemática.* Porto Velho: [s.n.], 2014. 166 p.

CAVALCANTI, J. D. B. *As tendências contemporâneas no ensino de Matemática e na pesquisa em Educação Matemática: questões para o debate.* 2010. Disponível em: <{http://www2.uesb.br/cursos/matematica/matematicavca/wp-content/uploads/dilson.pd}.>

CHEVALLARD, Y. *On didactic transposition theory: some introductory notes.* 1989.

DIAS, J. S. Mestrado Profissional em Matemática, *O Código da Mariner 9.* Alto Paraopeba: [s.n.], 2017. 23 p.

D'AMBROSIO, U. *Educação Matemática: Da teoria à prática.* Campinas: Papirus, 1996. 121 p.

EVES, H. *Introdução à história da matemática.* 5. ed. [S.l.]: Editora da Unicamp, 2011. 843 p.

FARIA, L. C. B. *Existências de códigos corretores de erros e protocolos de comunicação em sequências de DNA.* 322 p. Tese (Doutorado em Engenharia Elétrica) — Universidade Estadual de Campinas, Campinas, Campinas, 2011.

GLEICK, J. *A informação: Uma história, uma teoria, uma enxurrada.* São Paulo: Companhia das Letras, 2013. 521 p.

GUIMARÃES, W. P. S. Mestrado em Engenharia Elétrica, *Corretores de Erros para gravação magnética.* Recife: [s.n.], 2003. 239 p.

HAMMING, R. Error detecting and error correcting codes. *Bell System Tech. Journal.*, v. 26, p. 147–160, 1950.

HARARI, Y. N. *Homo Deus: uma breve história do amanhã.* [S.l.]: Companhia das Letras, 2016. 443 p.

HEFEZ, A. *Aritmética.* Rio de Janeiro: SBM, 2014.

HEFEZ, A.; VILLELA, M. L. T. *Códigos Corretores de Erros.* Rio de Janeiro: IMPA, 2008. 216 p.

IFRAH, G. *Os números: a história de uma grande invenção.* [S.l.]: Globo, 2005. 367 p.

ISSACSON, W. *Os inovadores: uma biografia da revolução digital.* São Paulo: Companhia das Letras, 2014.

KENSKI, V. M. *Educação e Tecnologias: o novo ritmo da informação.* Campinas: Papirus, 2011. 133 p.

LIMA, E. L. *Matemática e ensino.* Rio de Janeiro: SBM, 2002. 207 p.

LIRA, E. H. C. de. Trabalho de conclusão do curso de Licenciatura em Matemática, *Mapas conceituais com vídeos: uma proposta para a avaliação na componente currícular Estruturas Algébricas.* Caruaru: [s.n.], 2015. 79 p.

MELO, E. C. de Souza Gomes de. Mestrado Profissional em Matemática, *Um pequeno retrato acerca do aprendizado de nosso sistema de numeração decimal.* Recife: [s.n.], 2017. 103 p.

MENEGHESSO, C. *Códigos Corretores de Erros.* São Carlos: [s.n.], 2012. 43 p.

MILIES, C. P. *A Matemática dos códigos de barras detectando erros.* [S.l.: s.n.], 2008.

MILIES, C. P. Breve introdução à teoria dos códigos corretores de erros. In: *Colóquio de Matemática da Região Centro-Oeste.* [S.l.: s.n.], 2009. p. 33.

MIRANDA, D. S. Mestrado Profissional em Matemática, *Códigos corretores de erros e empacotamento de discos.* Recife: [s.n.], 2013. 63 p.

NICOLETTI, E. R. Mestrado Profissional em Matemática, *Aplicações de Álgebra Linear aos Códigos Corretores de Erros e ao Ensino Médio.* Rio Claro: [s.n.], 2015. 71 p.

PERNAMBUCO. *Parâmetros Curriculares para a Educação Básica do Estado de Pernambuco: matemática.* Recife: Secretária de Educação, 2012. 145 p.

PERNAMBUCO. *Parâmetros na sala de aula: matemática ensino fundamental e médio.* Recife: Secretária de Educação, 2013. 214 p.

PERNAMBUCO. *Parâmetros de Formação Docente: Ciências da Natureza e Matemática.* Recife: Secretária de Educação, 2014. 252 p.

ROCHA, A. S. L. *Modelo de sistema de comunicações digital para o mecanismo de importação de proteínas mitocondriais através de códigos corretores de erros.* 165 p. Tese (Doutorado em Engenharia Elétrica) — Universidade Estadual de Campinas, Campinas, Campinas, 2010.

ROQUE, T. *História da matemática: uma visão crítica, desfazendo mitos e lendas.* Rio de Janeiro: Zahar, 2012. 511 p.

ROUSSEAU, C.; AUBIN, Y. S. *Matemática e atualidade, volume 1.* Rio de Janeiro: SBM, 2015. 256 p.

RUDDER, C. *Dataclisma.* Rio de Janeiro: BestSelle, 2015. 301 p.

SANTOS, J. P. dos. *Introdução à Teoria dos Números.* Rio de Janeiro: IMPA, 1998. 196 p.

SARAMAGO, J. *Ensaio sobre a cegueira.* São Paulo: Companhia das Letras, 1995. 310 p.

SBM. *Contribuição da SBM para a discussão sobre currículo de matemática: Ensino Fundamental II.* 2015. Disponível em: <{https://www.sbm.org.br/wp-content/uploads/2015/01/Discussao_Curricular_Ensino_Fundamental_II_PROPOSTA.pd}.>

SBM. *Contribuição da SBM para a discussão sobre currículo de matemática: Ensino Médio.* 2015. Disponível em: <{https://www.sbm.org.br/wp-content/uploads/2015/01/Contribui%C3%A7%C3%A3o_da_SBM_Ensino_Meio_FINAL.pd}.>

SBM. *Contribuição da SBM para a discussão sobre currículo de matemática: Licenciatura.* 2015. Disponível em: <{https://www.sbm.org.br/wp-content/uploads/2015/01/Contribui%C3%A7%C3%A3o_da_SBM_Licenciatura_FINAL.pd}.>

SHANNON, C. E. A mathematical theory of communication. *Bell System Technical Journal*, v. 27, p. 379–423, 1948.

SHINE, C. Y. *21 Aulas de Matemática Olímpica.* [S.l.]: SBM, 2009. 324 p.

SILVA, F. P. P. Mestrado em Relações Internacionais, *Novas missões e novas tecnologias: o papel do Governo Federal e a criação da DARPA na construção da estratégia de supremacia em Ciência Tecnologia Defesa dos Estados Unidos na Guerra Fria.* Campinas: [s.n.], 2014. 136 p.

SILVA, V. A. da. *Por que e para que aprender a matemática?* São Paulo: Cortez, 2009. 132 p.

SING, S. *Fermat's enigma: the epic quest to solve the world's greatest mathematical problem*. New York: Anchor Books, 1997. 315 p.

STEWART, I. *Concepts of Modern Mathematics*. New York: Dover Publications, 1995. 339 p.

STEWART, I. *17 Equações que mudaram o mundo*. Rio de Janeiro: Zahar, 2013. 404 p.

SÁ, C. C. d.; ROCHA, J. *Treze Viagens pelo Mundo da Matemática*. 2. ed. Rio de Janeiro: SBM, 2012. 607 p.

VALENTE, W. R. A criação da disciplina escolar matemática no brasil e seu primeiro livro didático. *Educação em Revista*, Belo Horizonte, v. 43, p. 173–187, Jun 2006.

VIEIRA, N. P.; MUNHOZ, S. J. *Guerra Fria: Desafios, Confrontos e Historiografia.* 2008. Disponível em: <{http://www.diaadiaeducacao.pr.gov.br/portals/pde/arquivos/2341-6.pdf}.>

Apêndices

APÊNDICE A – O código $C(15, 11)$ no Excel

Neste apêndice detalhamos a construção de um pequeno programa para trabalhar com o código de Hamming $C(15, 11)$ no Excel, o mesmo pode ser utilizado nas aulas da sequência didática como um auxílio para a melhor compreensão do funcionamento deste código. Para os interessados em utilizar ou até mesmo melhorar este programa, disponibilizamos o link para acesso ao mesmo na próxima nota de rodapé[1].

Os primeiros elementos construídos no programa foram as matrizes geradora e de paridade, respectivamente. Note que estas matrizes foram definidas anteriormente, no Exemplo 2.61, e que os números em azul na Figura 19, representam as matrizes I_{11} e I_4 e os números em vermelho, as matrizes A e B do Teorema 2.56.

Figura 19 – Matrizes geradora e de paridade

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1																
2		Matriz geradora														
3		1	0	0	0	0	0	0	0	0	0	0	1	0	0	0
4		0	1	0	0	0	0	0	0	0	0	0	1	0	1	0
5		0	0	1	0	0	0	0	0	0	0	0	0	1	1	0
6		0	0	0	1	0	0	0	0	0	0	0	1	1	1	0
7		0	0	0	0	1	0	0	0	0	0	0	1	0	0	1
8	G=	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1
9		0	0	0	0	0	0	1	0	0	0	0	1	1	0	1
10		0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
11		0	0	0	0	0	0	0	0	1	0	0	1	0	1	1
12		0	0	0	0	0	0	0	0	0	1	0	0	1	1	1
13		0	0	0	0	0	0	0	0	0	0	1	1	1	1	1
14																
15		Matriz de paridade														
16		1	1	0	1	1	0	1	0	1	0	1	1	0	0	0
17	H=	0	0	1	1	0	1	1	0	0	1	1	0	1	0	0
18		0	1	1	1	0	0	0	1	1	1	1	0	0	1	0
19		0	0	0	0	1	1	1	1	1	1	1	0	0	0	1
20																

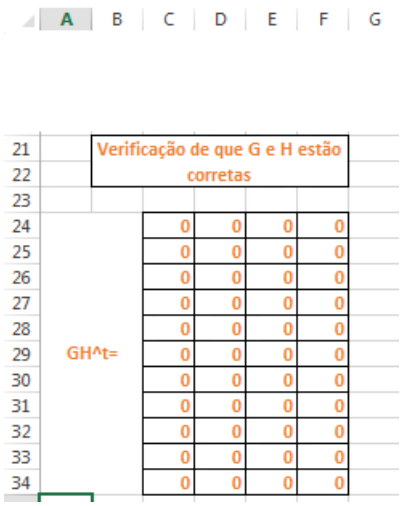
Fonte: O autor

Em seguida construímos a matriz que é igual ao produto das matrizes G_4 e H_4^t, a saber, $G_4H_4^t$ que pela teoria desenvolvida na Seção 2.6, deve ter como resultado a matriz nula, o resultado é mostrado na Figura 20.

Esta matriz serve para sabermos se, de fato estamos com as matrizes geradora e de paridade corretas, pois caso o produto em questão seja diferente da matriz nula, podemos concluir que houve um erro na escolha das matrizes geradora e de paridade. Por exemplo, suponha que por algum motivo, na célula $M1$ da matriz geradora tivéssemos trocado o

[1] Link: <https://www.dropbox.com/s/u3fjdq9xhs92qbb/C%C3%B3digo%20C%2815%2C11%29.xlsx?dl=0>

Figura 20 – Produto entre a matriz geradora e a transposta da matriz de paridade



Fonte: O autor

1 por um 0, e não tivéssemos colocado também um 1 na célula $A16$, como resultado o produto $G_4H_4^t$ não seria a matriz nula, o que nos levaria imediatamente à conclusão de que uma das matrizes, de paridade ou geradora, estava errada.

Para construír este produto de matrizes, escrevemos nas células de $C24$ à $F34$, o comando *MOD(expressão matemática; 2)* do Excel, em que MOD é a função congruência módulo um inteiro, a expressão matemática é a soma dos produtos das respectivas linhas de G_4 pelas respectivas colunas de H_4^t e o número 2 é o módulo que estamos considerando, assim, como resultado deste comando obteremos ou um 0 ou um 1, porém esperamos sempre obter um 0, pois isso indica que as escolhas de G_4 e H_4 que fizemos estão corretas. Por exemplo, para as duas primeiras e as duas últimas células desta matriz nós escrevemos:

- $C24 = MOD(B3 * B16 + C3 * C16 + D3 * D16 + E3 * E16 + F3 * F16 + G3 * G16 + H3 * H16 + I3 * I16 + J3 * J16 + K3 * K16 + L3 * L16 + M3 * M16 + N3 * N16 + O3 * O16 + P3 * P16; 2)$;
- $D24 = MOD(B3 * B17 + C3 * C17 + D3 * D17 + E3 * E17 + F3 * F17 + G3 * G17 + H3 * H17 + I3 * I17 + J3 * J17 + K3 * K17 + L3 * L17 + M3 * M17 + N3 * N17 + O3 * O17 + P3 * P17; 2)$;

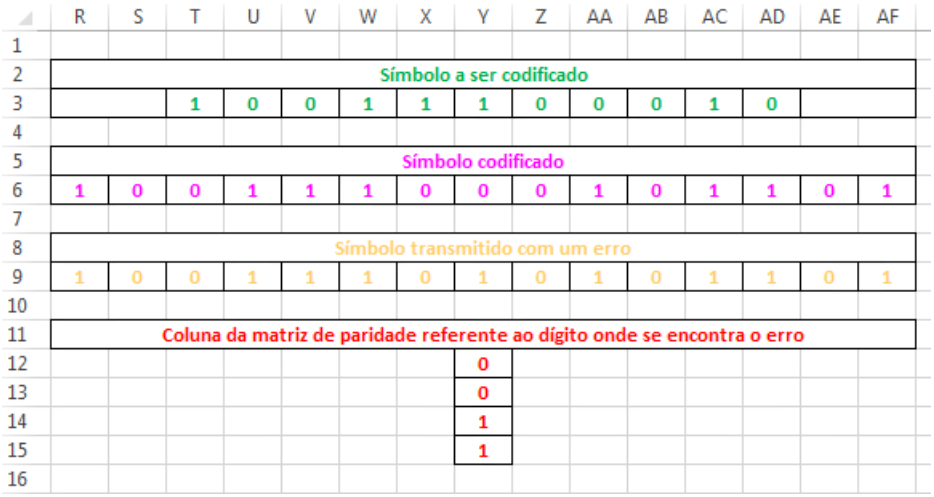
$\vdots$

- $E34 = MOD(B13 * B18 + C13 * C18 + D13 * D18 + E13 * E18 + F13 * F18 + G13 * G18 + H13 * H18 + I13 * I18 + J13 * J18 + K13 * K18 + L13 * L18 + M13 * M18 + N13 * N18 + O13 * O18 + P13 * P18; 2)$;

- $F34 = MOD(B13 * B19 + C13 * C19 + D13 * D19 + E13 * E19 + F13 * F19 + G13 * G19 + H13 * H19 + I13 * I19 + J13 * J19 + K13 * K19 + L13 * L19 + M13 * M19 + N13 * N19 + O13 * O19 + P13 * P19; 2)$.

Em seguida, construímos três linhas: uma para o símbolo que vai ser codificado; uma para o símbolo codificado; e uma para o símbolo contendo um único erro. O resultado está representado na Figura 21.

Figura 21 – Codificação e correção



Fonte: O autor

Os elementos do símbolo codificado na segunda linha são obtidos mais uma vez à partir do comando *MOD(expressão matemática; 2)*, só que agora a expressão matemática é a soma dos produtos das posições do símbolo a ser codificado pelas linhas da matriz geradora. Por exemplo, para as duas primeiras e as duas últimas células deste símbolo escrevemos:

- $R6 = MOD(T3 * M3 + U3 * M4 + V3 * M5 + W3 * M6 + X3 * M7 + Y3 * M8 + Z3 * M9 + AA3 * M10 + AB3 * M11 + AC3 * M12 + AD3 * M13; 2)$;
- $S6 = MOD(T3 * C3 + U3 * C4 + V3 * C5 + W3 * C6 + X3 * C7 + Y3 * C8 + Z3 * C9 + AA3 * C10 + AB3 * C11 + AC3 * C12 + AD3 * C13; 2)$;

$\vdots$

- $AD6 = MOD(T3 * O3 + U3 * O4 + V3 * O5 + W3 * O6 + X3 * O7 + Y3 * O8 + Z3 * O9 + AA3 * O10 + AB3 * O11 + AC3 * O12 + AD3 * O13; 2)$;

- $AF6 = MOD(T3 * P3 + U3 * P4 + V3 * P5 + W3 * P6 + X3 * P7 + Y3 * P8 + Z3 * P9 + AA3 * P10 + AB3 * P11 + AC3 * P12 + AD3 * P13; 2)$.

Note que o símbolo a ser codificado que aparece na Figura 21 é o mesmo utilizado no Exemplo 2.61. Semelhantemente, introduzimos um erro na 8ª posição e, como era de se esperar, obtivemos como resultado a 8ª coluna da matriz de paridade, acusando assim, a existência do erro na 8ª posição, da mesma forma que obtivemos no Exemplo 2.61. Com isso, encerramos a construção do código $C(15, 11)$ no Excel, bem como este apêndice.

APÊNDICE B – Material para a 1ª aula da sequência didática

Neste apêndice fazemos breves considerações sobre o funcionamento, a estrutura e os componentes básicos de um computador. Tais considerações tem por objetivo servir de material complementar para a realização da aula introdutória da nossa sequência didática e para isso, entendemos ser suficiente comentar de forma sucinta o funcionamento, a estrutura e os componentes básicos de um computador. Por motivo de organização, preferimos colocar este texto aqui neste apêndice e não no corpo da dissertação, porém entendemos que a leitura destas notas podem ser relegadas para um estudo mais aprofundado da sequência didática.

B.1 Material para a 1ª aula

Para início de conversa, notemos que um computador consiste basicamente em qualquer objeto que recebe uma informação como entrada, a processa e, em seguida, produz algum resultado como saída. Nosso cérebro, por exemplo, é uma espécie de computador[1]. Porém, ao falarmos em computadores aqui, estaremos no referindo ao nosso velho conhecido computador pessoal ou PC abreviação do inglês de *personal computer*, os quais, como citamos no texto referente às duas primeiras aulas da sequência didática, estão presentes em praticamente todos os lugares da nossa sociedade. Para uma caracterização mais detalhada do que consiste um PC, ver a referência na nota 1.

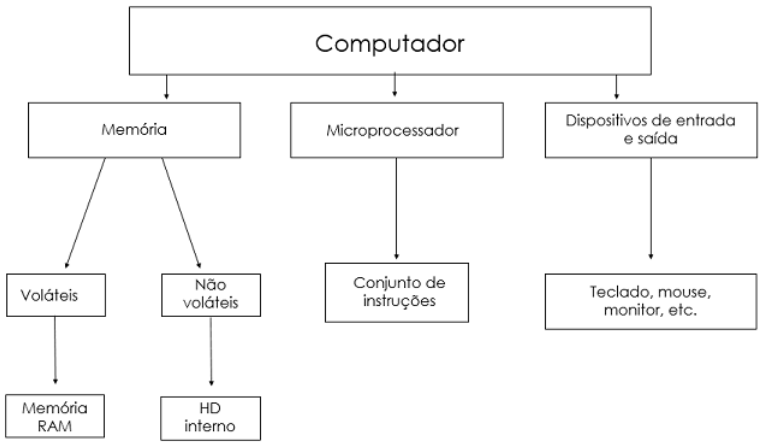
Embora à primeira vista possa parecer uma máquina altamente complexa, um computador é, em última análise, formado por três componentes básicos, a saber, *a memória, o microprocessador e os dispositivos de entrada e saída*[2] e esta estrutura básica pode ser reconhecida em inúmeras outras ferramentas tecnológicas como, por exemplo, um smartphone, uma calculadora ou uma televisão. A seguir entraremos em maiores detalhes sobre o que são e como funcionam cada um destes três componentes básicos.

- O microprocessador.

O microprocessador é um pequeno dispositivo eletrônico, mais precisamente, são chips com a aparência da Figura 23. Podemos dizer que o microprocessador é o centro

[1] <https://computer.howstuffworks.com/pc.htm>.
[2] <https://www.ime.usp.br/~elo/IntroducaoComputacao/Como%20funciona%20um%20computador.htm>

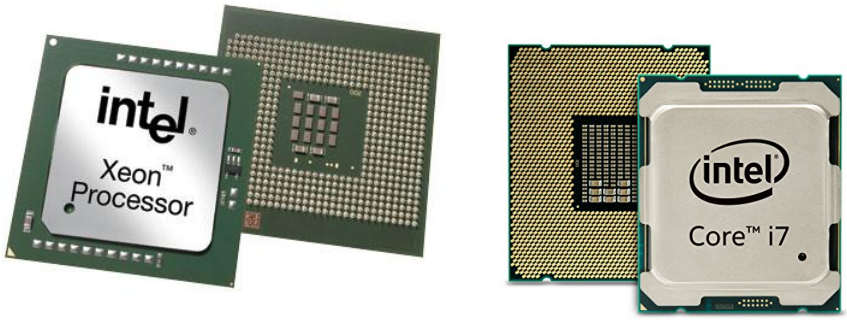
Figura 22 – Estrutura Básica de um computador



Fonte: O autor

nervoso do computador, pois é ele quem recebe e executa todos os comandos - lógicos e matemáticos diga-se de passagem - que são dados pelo sistema operacional (mais comumente, Windows, Linux e macOS) e pelos programas como, por exemplo, um editor de texto ou um reprodutor de videos durante o funcionamento da máquina. Uma boa ilustração para o papel do microprocessador no computador é a que o vê como o maestro de uma orquestra[3], o qual, supervisiona o trabalho dos músicos sob sua regência, marcando o passo e o ritmo corretos, o momento de cada instrumento atuar e silenciar, dentre outras coisas, tudo isso com vistas ao bom funcionamento do concerto.

Figura 23 – O microprocessador



Fonte: Google Images

- A memória.

[3] <http://www.di.ufpb.br/raimundo/PCaFundo/cpu/mp.htm>

Damos o nome genérico de mémoria de um computador, ao conjunto formado por todos os componentes que permitem o armazenamento de dados no mesmo. Segundo a referência da nota 1, a memória de um computador pode ser classificada em dois grupos: as memórias *voláteis* e as memórias *não voláteis.*

As memórias voláteis atuam enquanto o computador está em funcionamento, ou seja, ligado, um exemplo típico de memória volátil é a chamada memória RAM - *Random access memory* ou Memória de Acesso Aleatório. A memória RAM funciona armazenando e processando os dados presentes nos aplicativos e programas em funcionamento no computador. Assim, se uma pessoa estiver editando um texto no Word, por exemplo, e o computador é por algum motivo desligado antes que o texto tenha sido salvo, o texto não salvo será perdido, pois ainda estava armazenado apenas na memória RAM do computador.

A relação entre a memória RAM e o microprocessador funciona de forma semelhante a um garçom (memória RAM) que apreseta a um cliente (o microprocessador), um cardápio com um conjunto de opções disponíveis oferecidas pelo restaurante. Basta o cliente fazer uma escolha que o garçom se encarregará de fornecer o pedido desejado para a ocasião, seja ela um almoço ou jantar, por exemplo. Feito seu papel o garçom se retira e só se apresenta novamente a sua mesa quando solicitado, seja para a conta ou para um cafezinho ou a sobremesa após a refeição principal. Evidentemente, o garçom dispõe de informações relacionadas com a atividade em questão como, por exemplo, o sexo, a cor e a constituição física do cliente, porém informações anteriores à entrada no restaurante como, por exemplo, o nome do cliente, a condução em que chegou ou a senha da sua conta bancária não estão disponíveis para o garçom.

As memórias não voláteis, dentre as quais, destaca-se a memória ROM - *Read Only Memory* ou Memória Apenas de Leitura, são permanentes, ou seja, não são perdidas toda vez que o computador não está funcionando. Na memória ROM de um PC está um programa fundamental para o funcionamento do mesmo, chamado BIOS - *Basic Input Output System* ou Sistema Básico de Entrada e Saída, o qual é o responsável pela inicialização da máquina quando apertamos o botão de ligar. Além disso, a ROM armazena informações que não podem ser apagadas, mas apenas lidas (como o nome já sugere), dessa forma, lembrando o exemplo anterior do garçom e restaurante, ela funcionaria como o nome do restaurante ou o seu horário de funcionamento ou o local onde ele se encontra.

- Dispositivos de entrada e saída.

Se não fossem os dispositivos de entrada e saída, provavelmente os computadores não seriam o que são hoje nem estariam amplamente difundidos como o são. O teclado, o monitor, as caixas de som, entradas USB, dentre outros são apenas alguns dos muitos dispositivos de entrada e saída de um computador, os quais nos permitem facilmente introduzir dados, receber e interpretar os resultados gerados pela máquina. Alguns dispositivos

como caixas de som, monitor e datashow são ditos de saída, pois não podem fornecer dados à máquina, mas apenas os receber. Já o mouse, o teclado e o microfone são dispositivos de entrada, pois são através deles que fornecemos os dados que a máquina processará. Por fim, existem dispositivos ditos hibridos que além de entrada também são de saída, este é o caso das impressoras multifuncionais e pendrives, por exemplo, ver Figura 24.

Figura 24 – Alguns dispositivos de entrada e saída.

Fonte: Google Images

Com isso, encerramos o que entendemos ser um explicação introdutória e elementar do que seja um computador, a qual o professor pode recorrer se achar necessário. Para abordagens mais detalhadas e aprofundadas o professor pode consultar as referências nas notas de rodapé 1,2 e 3, as quais em parte utilizamos para a realização deste apêndice.