UNIVERSIDADE ESTADUAL DE CAMPINAS

Faculdade de Engenharia Elétrica e de Computação

Gustavo Terra Bastos

Códigos de Subespaço Geometricamente Uniformes e uma Proposta de Construção de Redes Quânticas

Campinas

2017

Gustavo Terra Bastos

Códigos de Subespaço Geometricamente Uniformes e uma Proposta de Construção de Redes Quânticas

Tese apresentada à Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em Engenharia Elétrica, na Área de Telecomunicações e Telemática.

Orientador: Prof. Dr. Reginaldo Palazzo Junior

Este exemplar corresponde à versão final da tese defendida pelo aluno Gustavo Terra Bastos, e orientada pelo Prof. Dr. Reginaldo Palazzo Junior

---

Campinas

2017

Agência(s) de fomento e nº(s) de processo(s): CNPq, 142094/2013-7; CAPES

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca da Área de Engenharia e Arquitetura
Luciana Pietrosanto Milla - CRB 8/8129

B297c

Bastos, Gustavo Terra, 1986-
Códigos de subespaço geometricamente uniformes e uma proposta de construção de redes quânticas / Gustavo Terra Bastos. – Campinas, SP : [s.n.], 2017.

Orientador: Reginaldo Palazzo Junior.
Tese (doutorado) – Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Códigos corretores de erros (Teoria da informação). 2. Comunicação quântica. I. Junior, Reginaldo Palazzo,1951-. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Geometrically uniform subspace codes and a proposal to construct quantum networks
Palavras-chave em inglês:
Error correcting codes (Information theory)
Quantum communication
Área de concentração: Telecomunicações e Telemática
Titulação: Doutor em Engenharia Elétrica
Banca examinadora:
Reginaldo Palazzo Junior [Orientador]
Agnaldo José Ferrari
Fernando Eduardo Torres Orihuela
Giuliano Gadioli La Guardia
Marines Guerreiro
Data de defesa: 22-06-2017
Programa de Pós-Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE DOUTORADO

Candidato: Gustavo Terra Bastos
RA: 143800

Data da Defesa: 22 de junho de 2017

Título da Tese: "Códigos de Subespaço Geometricamente Uniformes e uma Proposta de Construção de Redes Quânticas"

Prof. Dr. Reginaldo Palazzo Junior (Presidente, FEEC/UNICAMP)
Prof. Dr. Agnaldo José Ferrari (FC/UNESP)
Prof. Dr. Fernando Eduardo Torres Orihuela (IMECC/UNICAMP)
Prof. Dr. Giuliano Gadioli La Guardia (DEMAT/UEPG)
Prof. Dra. Marines Guerreiro (DMA/UFV)

A ata de defesa, com as respectivas assinaturas dos membros da Comissão Julgadora, encontra-se no processo de vida acadêmica do aluno.

Dedico esta tese aos meus pais Arlindo e Luiza e a minha esposa Mariela.

Agradecimentos

Em primeiro lugar, gostaria de agradecer a Deus por se fazer presente sempre em minha vida e pelas bênçãos constantes que me foram e são concedidas. Graças a Ele, com certeza, posso ter o prazer de concluir este trabalho.

Agradeço aos meus pais Arlindo e Luiza por todo o sacrifício em prol do bem-estar e da educação de qualidade que ofertaram aos seus filhos. Muito obrigado pelo amor e carinho incondicionais. Aos meus irmãos Felipe e André, obrigado pelo companheirismo e pelos bons momentos juntos.

À minha esposa Mariela, por me acompanhar desde a graduação, quando a conquista materializada neste trabalho não passava de um sonho. Obrigado por sempre acreditar no meu potencial, por todo carinho, amor e compreensão, mesmo nos momentos mais difíceis. Essa conquista só foi possível porque tive você ao meu lado, sempre.

Ao professor Palazzo, obrigado por me tornar um pesquisador em formação, compartilhando seu conhecimento, vivência e experiências profissionais em nossas agradáveis reuniões.

Aos professores que compõem a banca, pelas valiosas sugestões e por aceitarem o convite.

Aos meus amigos de Varginha, Campestre, Viçosa e Campinas, dentre outras cidades, por tornarem a caminhada em busca deste objetivo bem mais suave.

A todos os meus antigos mestres, por fazerem parte da minha formação como profissional.

Finalmente, agradeço a CAPES e o CNPQ pelo suporte financeiro.

"O que eu faço é uma gota no meio de um oceano. Mas sem ela, o oceano será menor."
(Madre Teresa de Calcutá)

Resumo

Códigos de subespaço se mostram muito úteis contra a propagação de erros em uma rede linear *multicast*. Em particular, a família dos códigos de órbita apresenta uma estrutura algébrica bem definida o que, possivelmente, resultará na construção de bons algoritmos de decodificação e uma forma sistemática para o cálculo dos parâmetros do código.

Neste trabalho, apresentamos um estudo dos códigos de órbita vistos como códigos geometricamente uniformes. A caracterização destas duas classes segue direto da definição de códigos de órbita e, dado um particionamento geometricamente uniforme destes códigos a partir de subgrupos normais do grupo gerador, propomos uma redução sobre o número de cálculos necessários para a obtenção das distâncias mínimas de um código de órbita abeliano e de um código L-nível, além de um algoritmo de decodificação baseado nas regiões de Voronoi.

No último capítulo deste trabalho, propomos uma ideia de como projetar, do ponto de vista teórico, uma possível rede capaz de transmitir e operar informações quânticas. Tais informações são representadas por estados quânticos emaranhados, onde cada ket destes estados está associado a um subespaço vetorial.

Palavras-chaves: Códigos Geometricamente Uniformes; Códigos de Órbita; Redes Quânticas.

Abstract

Subspace codes have been very useful to solve the error propagation in a multicast linear network. In particular, the orbit codes family presents a well-defined algebraic structure, which it will probably provide constructions of good decoding algorithms and a systematic way to compute the parameters of the code.

In this work, we present a study of orbit codes seen as geometrically uniform codes. The characterization of both classes is direct from the definition of orbit codes and, given a uniform geometrically partition of these orbit codes from their normal subgroups of the generator group, we propose a reduction of the computation necessary for obtaining the minimum distances of an abelian orbit code and an L-level code, in addition to a decoding algorithm based on Voronoi regions.

In the last chapter, we propose a hypothetical quantum network coding for the transmission of quantum information. This network consists of maximum entangled pure quantum states such that each ket of these states is associated with a vector subspace.

Keywords: Geometrically Uniform Codes; Orbit Codes; Quantum Networks.

Lista de Figuras

Lista de Tabelas

Sumário

1 Introdução

Em um passado não muito distante, era comum que uma rede de transmissão de informações fosse descrita como um conjunto de nós intermediários conectando fonte ao destinatário, onde os nós intermediários tinham a função de selecionar, replicar ou repassar as informações transmitidas pela fonte, isto é, tais nós agiam simplesmente como comutadores. Uma rede é dita *unicast* quando um dado nó é conectado apenas a um outro nó. Caso contrário, se um dado nó é conectado por duas ou mais arestas a dois ou mais nós, então dizemos que a rede é *multicast*. Neste trabalho consideramos apenas o caso *multicast*.

Em (AHLSWEDE N. CAI, 2000) os autores propuseram que os nós intermediários de uma rede não atuassem apenas como comutadores, mas sim codificadores (codificação interna), onde estes nós seriam capazes de executar as mesmas tarefas de um nó comutador, além de poderem processar os pacotes de informações recebidos, de forma a otimizar a transferência desses pacotes para os demais nós intermediários. Aqui, considera-se uma informação como sendo um vetor de $\mathbb{F}_q^n$, e o processamento desenvolvido pelos nós intermediários como combinações lineares desses vetores. Quando os nós desenvolvem combinações lineares aleatórias, dizemos que estes nós executam codificação de rede aleatória ou não coerente. O exemplo descrito no próximo parágrafo ilustra a situação teórica mais usual de uma rede linear não coerente.

Considere a rede *multicast* conhecida como rede borboleta, onde os canais (arestas) transmitem até um bit de informação por unidade de tempo e não sofrem a ação de qualquer ruído. Nesta rede há uma fonte (F) e dois destinatários (D_1 e D_2) e deseja-se enviar as informações m_1 e m_2 para ambos destinatários. Suponha, inicialmente, que esta rede não admita codificação interna, ou seja, os nós intermediários não podem processar as informações recebidas, mas atuam apenas como comutadores. Este caso é ilustrado pela Figura 1.

No primeiro instante de tempo ($t = 1$), a fonte distribui as informações para os nós 1 e 2, que repassam as mesmas para D_1, 3 e D_2. No segundo instante de tempo ($t = 2$), o nó 3 dispõe de ambas informações, mas apenas uma delas poderá ser repassada para o nó 4. Sem perda de generalidade, primeiramente, a mensagem m_1 será repassada para o nó 4 e, em seguida, para o destinatário D_2. No terceiro instante de tempo ($t = 3$), a outra informação, m_2, é então entregue ao nó 4 e, por fim, ao destinatário D_1. Assim, foram necessários três instantes de tempo para que as informações fossem ambas entregues aos destinatários.

Agora, vamos descrever o contexto onde os nós da rede borboleta podem codificar

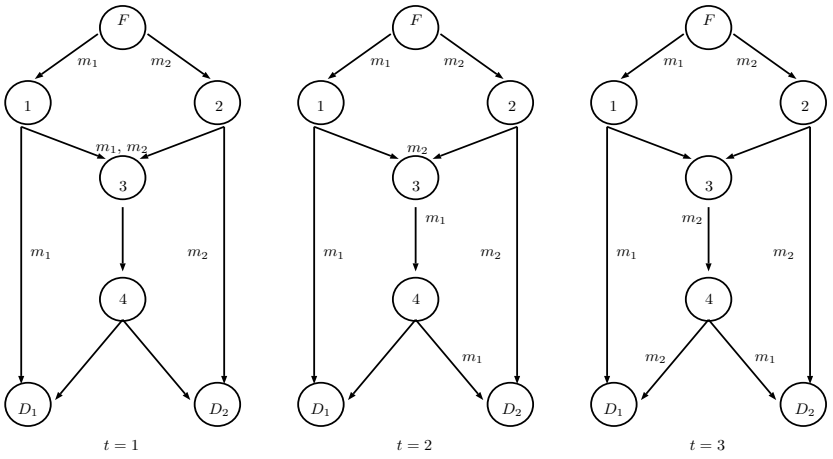


Figura 1 – Rede borboleta sem codificação

as informações recebidas. Este caso é ilustrado pela Figura 2.

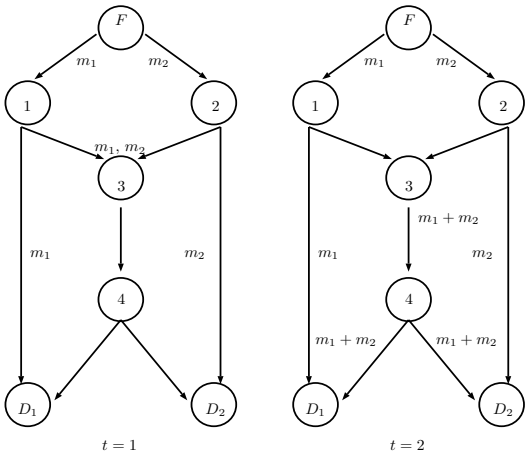


Figura 2 – Rede borboleta com codificação

No primeiro instante de tempo ($t = 1$), a rede processa de forma análoga como foi descrito na situação em que os nós não são codificadores, ou seja, a fonte distribui as mensagens m_1 e m_2 para os nós 1 e 2, que as encaminham para os nós D_1, 3 e D_2. Já no segundo instante de tempo ($t = 2$), e aqui o fato dos nós intermediários serem aptos a processar as informações fará toda a diferença, o nó 3 pode processar as mensagens m_1 e m_2 como a mensagem $m_1 + m_2$, e encaminhar esta nova mensagem para o nó 4, que em seguida a encaminha para os nós D_1 e D_2. Neste ponto, a partir de uma operação semelhante à operação lógica *xor*, os nós destinatários são capazes de recuperar as informações que ainda não receberam, isto é, D_1 consegue recuperar a mensagem m_2 e o nó D_2 recupera m_1. Portanto, neste caso, verifica-se que foram necessários apenas dois instantes de tempo para que ambos destinatários pudessem receber as informações m_1 e m_2, e isso comprova a eficiência do uso de codificação para a transmissão de informações em redes *multicast*.

Agora, consideremos uma situação real, em que diversas ações podem comprome-

ter a segurança da informação originalmente transmitida pela fonte. Dentre estas ações, podemos citar apagamentos e atrasos no envio das mensagens, além de agentes maliciosos infiltrados nos nós. Assim, apesar do ganho no uso de codificação visto nos parágrafos anteriores, em contrapartida, uma rede linear é extremamente sensível à propagação de erros. De fato, suponha que um dos canais (seta vermelha pontilhada) sofreu a ação de um ruído. Conforme é exposto na Figura 3, os pacotes de informações recebidos por um nó, oriundos deste canal ruidoso, serão codificados com outros pacotes, gerando novas mensagens corrompidas e, assim, toda a transmissão será comprometida.

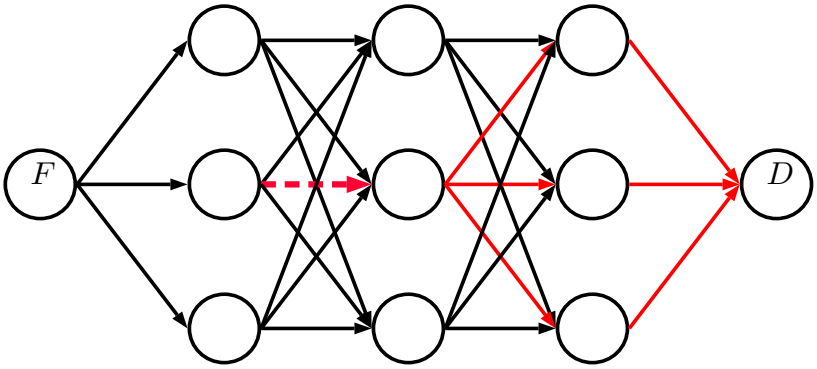


Figura 3 – Rede corrompida

Para combater esse problema, foi proposto um esquema de codificação de redes (externa), onde considera-se uma escolha adequada dos pacotes de informações que serão injetados na rede. De forma bastante simples, seja M um pacote de informações enviado para a rede, N as combinações lineares aleatórias executadas pelo nó e um erro (E) ocorrido durante a transmissão. A Figura 4 descreve esta situação.

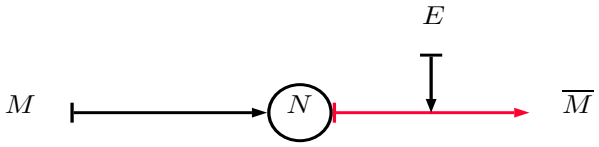


Figura 4 – Erro ocorrido durante uma transmissão

Em (KöTTER, 2008), os autores consideraram o pacote de informações M, que é uma coleção de vetores de $\mathbb{F}_q^n$, como o espaço vetorial gerado por esses vetores (esse espaço vetorial é descrito pelo espaço linha de uma matriz cujas linhas são tais vetores e, por abuso de notação, também denotaremos tal matriz por M) e, na ausência de erros, como a matriz NM é uma $\mathbb{F}_q-$combinação linear das linhas da matriz M, então tem-se o mesmo espaço vetorial, isto é, os espaços linha das matrizes M e NM são os mesmos. Por outro lado, se considerarmos a presença do erro E, obteremos um espaço vetorial $\overline{M} = NM + E$, diferente daquele gerado por M.

Para superar a presença de erros e apagamentos inseridos pela ação do canal, deve-se fazer uma escolha adequada do conjunto de pacotes de informações enviados, isto é, do

conjunto de espaços vetoriais gerados por cada um destes pacotes, de forma a detetar um possível erro gerado na saída de um nó, ou seja, um espaço vetorial que não pertence ao conjunto inicial de espaços vetoriais. Este conjunto de espaços vetoriais é dito um *código de subespaço*.

1.1 Apresentação do Problema

Neste trabalho propomos, com base no modelo de canal e nos códigos de subespaço descritos em (KöTTER, 2008), apresentar um estudo mais aprofundado sobre a estrutura dos códigos de órbita, que foram inicialmente propostos por (TRAUTMANN F. MANGANIELLO, 2010), pois trata-se de uma família de códigos de subespaço com uma rica estrutura algébrica, o que é altamente desejado, pois pode-se conjecturar a projeção de códigos de forma bastante ordenada, além do fato de que esta estrutura poderá ser explorada para a descrição de bons algoritmos de decodificação, utilizando técnicas algébricas bastante sólidas e a vasta literatura sobre o assunto.

Com base nas propostas de construções e resultados oriundos dos trabalhos de (G.-LUERSSEN K. MORRISON, 2015; TRAUTMANN F. MANGANIELLO, 2013), que se distinguem por apresentarem diferentes representações para os subespaços vetoriais de uma dada grassmanniana, buscamos analisar a estrutura dos códigos de órbita de um ponto de vista mais micro, isto é, a partir dos seus subcódigos de órbitas, onde informações valiosas sobre os códigos de órbita podem ser extraídas. Pudemos verificar que os códigos de órbita, vistos no contexto de códigos de subespaço, são os equivalentes aos códigos geometricamente uniformes, propostos por (JR., 1991) no início dos anos 90. Esta classe de códigos encantou toda a comunidade acadêmica devido ao fato de aliar estruturas algébrica e geométrica bastante sólidas, além de uma disposição das palavras código bastante simétrica, o que implica em diversas propriedades desejadas na projeção de sistemas de comunicações. Apenas como uma justificativa para toda esta expectativa gerada pelos códigos geometricamente uniformes, a partir de uma análise sobre as propriedades locais de uma dada palavra código, estas podem ser estendidas para cada uma das demais palavras código, o que implica, por exemplo, poder afirmar que todas as palavras código destes códigos possuem a mesma probabilidade de erro.

Em um primeiro momento, propomos apresentar um estudo sobre os códigos de órbita vistos como códigos geometricamente uniformes. Isso implica em expor algumas definições oriundas da teoria clássica de códigos corretores de erros como perfis de distância global e regiões de Voronoi para o contexto de códigos de subespaço. Também abordamos neste trabalho um estudo sobre partições de códigos de órbita a partir de uma ação gerada por um grupo quociente. Logo, neste caso, é necessário entendermos quais condições devem ser satisfeitas para que um subgrupo do grupo gerador da órbita seja normal. Al-

guns resultados da literatura nos fornecem essas condições e, assim, podemos apresentar uma análise completa sobre particionamentos geometricamente uniformes resultando, por exemplo, em uma redução considerável do número de cálculos necessários para a obtenção da distância mínima dos códigos de órbita gerados por grupos abelianos. Além disso, com base no conceito de regiões de Voronoi, exibimos um algoritmo de decodificação para códigos de órbita. Finalizando esta primeira parte do problema relacionado ao estudo dos códigos de órbita, novamente, fazendo uso das partições geometricamente uniformes, descrevemos uma forma sistemática para a construção de códigos L-nível onde, novamente, a partir da caracterização dos códigos de órbita como códigos geometricamente uniformes, nos garante uma redução do número de cálculos necessários para a descrição da distância mínima projetada para o código L-nível.

No último capítulo deste trabalho, abordamos uma outra área de pesquisa também relacionada com a transmissão de informações. Trata-se da teoria da informação quântica. De forma bastante superficial, diversas pesquisas apontam a eficiência no uso de estados quânticos nos processos de transmissão e proteção da informação, em comparação aos meios tradicionais, apesar do fato de que o homem ainda não possui um completo entendimento sobre esta “nova"mecânica. Vale citar, como exemplo, o fato de que o computador quântico desenvolve um número muito maior de operações por unidade de tempo, quando comparado aos computadores clássicos, e será capaz de decifrar quaisquer mensagens criptografadas via o método de cifragem RSA, que é um dos mais populares hoje em dia. Um dos fatores que contribuem para essa eficiência reside em uma característica própria destes estados conhecida como emaranhamento quântico.

Outra contribuição desta tese é a apresentação de definições básicas da mecânica quântica necessárias para o entendimento da medida de emaranhamento quântico de Meyer e Wallach, via a releitura proposta por (GAZZONI, 2008). Esta releitura propõe uma forma de como medir se um estado quântico puro é ou não emaranhado, a partir da análise dos códigos binários clássicos que podem ser extraídos do estado quântico puro em questão. Como estados quânticos puros emaranhados são altamente desejáveis em comunicações, propomos neste trabalho uma ideia embrionária de como podemos aliar códigos de subespaço com o contexto da teoria da informação quântica. Assim, com base em uma situação inicial de uma rede borboleta “quântica", apresentamos uma forma bastante sólida de como associar subespaços vetoriais aos kets de um estado quântico puro emaranhado, e como os nós desta provável rede devem operar os subestados transmitidos, com base nos subespaços vetoriais associados.

1.2 Organização do Trabalho

Este trabalho está organizado da seguinte forma: No Capítulo 2, apresentamos a fundamentação matemática básica para o entendimento necessário das estruturas algébricas conhecidas como grupos e corpos finitos, que são constantemente usadas durante a exposição deste trabalho, além de uma revisão de conceitos de geometria projetiva e, em particular, do Teorema Fundamental da Geometria Projetiva, que são fundamentais para a descrição do espaço ambiente/métrico donde extrairemos os códigos propostos no Capítulo 3 e o entendimento das isometrias que agem neste espaço, que serão importantes para o Capítulo 4.

No Capítulo 3, inicialmente descrevemos o modelo de canal para redes proposto em (KöTTER, 2008), e que será considerado durante todo o trabalho. Para esse canal, apresentamos os códigos corretores de erros utilizados, que são conhecidos como códigos de subespaço, e diversos resultados relacionados aos limitantes para os parâmetros destes códigos. De interesse para uma das contribuições deste trabalho, dedicamos grande parte deste capítulo para a família dos códigos de órbita, apresentando as duas "diferentes"representações para estes códigos e os seus principais resultados, com base nos trabalhos de (G.-LUERSSEN K. MORRISON, 2015; TRAUTMANN F. MANGANIELLO, 2013). Por fim, com base no trabalho de (BARDESTANI, 2015), uma construção de códigos de órbita vistos como uma união de códigos de órbita cíclicos é apresentada, dado que o grupo gerador destes códigos é descrito com base em dois subgrupos constantemente usados nesta tese.

No Capítulo 4, apresentamos as nossas primeiras contribuições. Dadas as definições clássicas de códigos gerados por grupos e códigos geometricamente uniformes, verificamos que, para o caso de códigos de dimensão constante, estas definições coincidem com a definição de códigos de órbita. Assim, de posse de alguns conceitos clássicos como regiões de Voronoi e partições geometricamente uniformes, vistos no contexto de códigos de subespaço, apresentamos uma forma de como reduzir o número de cálculos necessários para obtermos a distância mínima dos códigos de órbita gerados por grupos abelianos e, em particular, dos códigos de órbita cíclicos. Mais ainda, apresentamos um exemplo de como podemos usar as regiões de Voronoi para decodificar corretamente uma mensagem recebida e, finalmente, mostramos como a codificação multinível para códigos de subespaço proposta por (NóBREGA, 2009) pode ser otimizada para o caso de códigos de órbita.

No Capítulo 5, apresentamos nossa segunda contribuição para este trabalho. Dado um embasamento superficial sobre os fundamentos básicos da mecânica quântica, propomos uma forma de como relacionar subespaços vetoriais aos kets de um estado quântico puro emaranhado, cuja classificação como estado emaranhado segue uma releitura da medida proposta por Meyer e Wallach dada por (GAZZONI, 2008). Esta associação entre subespaços vetoriais e subestados quânticos de um estado quântico puro emaranhado abre

a possibilidade de se considerar redes lineares transmissoras de informações quânticas, algo ainda não visto na literatura da área. A nossa proposta é formalizada e explicitada a partir de uma rede quântica similar à rede borboleta.

2 Preliminares Algébricos

Para o estudo de códigos de subespaço geometricamente uniformes ou, conforme será visto adiante, para o estudo de códigos (de subespaço) de órbita, se faz necessário a definição de conceitos básicos da teoria de grupos como, por exemplo, grupos quocientes, ações de grupo e produto semi-direto de grupos, além de resultados relacionados à definição, construção e representação de corpos finitos, que podem ser vistos como espaços vetoriais de dimensão finita, e que são muito úteis para os diversos cálculos e exemplos propostos neste trabalho.

O espaço projetivo é o ambiente onde definiremos os códigos de subespaço e as aplicações que preservam distância neste espaço, e estão diretamente relacionadas com o conceito de códigos geometricamente uniformes, são conhecidas como isometrias.

Na Seção 2.1 apresentamos os conceitos básicos de álgebra necessários para este trabalho.

Na Seção 2.2, faremos uma breve revisão de alguns conceitos da teoria de códigos corretores de erros clássicos, que serão necessários para o resultado proposto no Capítulo 5.

Por fim, a Seção 2.3 é destinada à descrição do espaço ambiente de onde extrairemos os códigos propostos neste trabalho, isto é, a geometria ou espaço projetivo, além da apresentação de um resultado conhecido como Teorema Fundamental da Geometria Projetiva, o qual é essencial para uma das propostas deste trabalho.

2.1 Grupos, Anéis e Corpos

De acordo com a definição que será vista no próximo capítulo, códigos de órbita (ou códigos geometricamente uniformes) possuem uma estrutura algébrica e geométrica muito sólida, devido a ação de grupos sobre espaços vetoriais de dimensão finita. Assim, nesta seção, descreveremos vários resultados importantes da álgebra relacionados a teoria de grupos e anéis (em particular, corpos finitos).

As principais referências que norteiam esta seção são (LIDL, 1997; ROTMAN, 1995).

2.1.1 Grupos

Definição 2.1.1. *Um* grupo *é um conjunto* $(G, \cdot)$ *com uma operação binária* $\cdot$ *sobre* G *tal que as seguintes três propriedades valem:*

(i) $\cdot$ *é associativa, isto é, para quaisquer* $a, b, c \in G$,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(ii) Existe um elemento identidade e *em* G *tal que, para todo* $a \in G$,

$$a \cdot e = e \cdot a = a.$$

(iii) Para cada $a \in G$, *existe um elemento inverso* $a^{-1} \in G$ *tal que*

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

Se o grupo também satisfaz

(iv) Para todos $a, b \in G$,

$$a \cdot b = b \cdot a,$$

então G *é um* grupo abeliano.

Definição 2.1.2. *Um subconjunto* H *do grupo* G *é um subgrupo de* G *se* H *é ele próprio um grupo com respeito à operação de* G. *Neste caso, denotaremos* $H \leq G$.

Se H é um subgrupo do grupo G e $t \in G$, então uma classe lateral à direita de H em G corresponde ao subconjunto

$$Ht = \{ht : h \in H\}, \tag{2.1}$$

onde t é um representante desta classe. Analogamente, define-se a classe lateral à esquerda de H em G

$$tH = \{th : h \in H\}. \tag{2.2}$$

Teorema 2.1.3. *(ROTMAN, 1995) Se* H *é um subgrupo de* G, *então o número de classes à direita de* H *em* G *é igual ao número de classes à esquerda de* H *em* G.

O conjunto das classes laterais (à direita ou à esquerda) de H em G é denotado por G/H e o número de tais classes é dito índice de H em G, e será denotado por $[G : H]$.

Definição 2.1.4. *Um subgrupo* $H \leq G$ *é um subgrupo normal de* G, *denotado por* $H \lhd G$, *se* $g \cdot H \cdot g^{-1} \in H$, *para todo* $g \in G$.

Quando $H \lhd G$, então as classes laterais à esquerda e à direita de H em G são iguais, isto é, dado $t \in G$, tem-se $Ht = tH$.

Teorema 2.1.5. *(ROTMAN, 1995) Se* $H \lhd G$, *com* G *um grupo finito, então as classes laterais de* H *em* G *formam um grupo, denotado por* G/H, *de ordem* $[G : H] = |G|/|H|$.

O grupo definido no Teorema 2.1.5 é dito grupo quociente, e desempenhará um papel fundamental nos resultados propostos neste trabalho.

Definição 2.1.6. *Um grupo multiplicativo G é dito ser cíclico se existe um elemento $a \in G$ tal que, para qualquer $b \in G$, existe algum inteiro j com $b = a^j$. Tal elemento é chamado um gerador do grupo cíclico e escrevemos $G = \langle a \rangle$.*

Exemplo 2.1.7. *Consideremos o grupo diedral D_n, que corresponde às simetrias de um polígono de n lados. Este grupo tem a seguinte apresentação*

$$D_n := \left\langle a, b : a^n = b^2 = e, bab = a^{-1} \right\rangle.$$

As simetrias do quadrado (elementos do D_4) podem ser representadas pelas seguintes matrizes

$$D_4 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}.$$

A seguir, apresentamos dois subgrupos de D_4. O subgrupo

$$H_1 = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle \tag{2.3}$$

representa o conjunto das rotações por inteiros múltiplos de 90° e o subgrupo

$$H_2 = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \tag{2.4}$$

representa o conjunto das reflexões sobre ambos os eixos.

Definição 2.1.8. *Sejam $(G, \cdot)$ e $(H, *)$ dois grupos. Uma aplicação $f : G \to H$ é um homomorfismo de grupos se, para todos $a, b \in G$, vale*

$$f(a \cdot b) = f(a) * f(b).$$

Um isomorfismo é um homomorfismo que também é uma bijeção. Dizemos que G é isomorfo a H, e denotamos por $G \simeq H$, se existir um isomorfismo $f : G \to H$.

Definição 2.1.9. *Se X é um conjunto e G é um grupo, então X é um $G-$conjunto se existe uma aplicação $\lambda : G \times X \to X$ (dita uma* ação à esquerda*), em que $\lambda : (g, x) \mapsto gx$, tal que*

(i) $ex = x$, para todo $x \in X$.

(ii) $g(hx) = (g \cdot h)x$, *para todos* $g, h \in G$ *e* $x \in X$.

Também dizemos que G age *sobre* X. *Se* $|X| = n$, *então* n *é dito o grau do* $G-$*conjunto* X.

Dados o grupo G e o conjunto X, podemos também definir uma ação de G sobre X à direita.

Existem dois conceitos fundamentais relacionados a um G-conjunto.

Definição 2.1.10. *Se* X *é um* G*-conjunto e* $x \in X$, *então a* $G-$*órbita de* x, *ou simplesmente a* órbita *de* x, *é o conjunto*

$$\mathcal{O}(x) := \{gx : g \in G\} \subseteq X. \tag{2.5}$$

As órbitas de X formam uma partição do conjunto X. De fato, dados $x, y \in X$, a relação $x \sim y \Leftrightarrow \exists g \in G : y = gx$ é uma relação de equivalência.

Definição 2.1.11. *Se* X *é um* $G-$*conjunto e* $x \in X$, *então o* estabilizador *de* x, *denotado por* $Stab_G(x)$, *é o subgrupo*

$$Stab_G(x) := \{g \in G : gx = x\} \leq G. \tag{2.6}$$

Teorema 2.1.12. *(ROTMAN, 1995) Se* X *é um* G*-conjunto e* $x \in X$, *então*

$$|\mathcal{O}(x)| = [G : Stab_G(x)],$$

onde $[G : Stab_G(x)]$ *descreve o índice de* $Stab_G(x)$ *em* G.

Corolário 2.1.13. *(ROTMAN, 1995) Se um grupo finito* G *age sobre um conjunto* X, *então o número de elementos em qualquer órbita é um divisor de* $|G|$.

Definição 2.1.14. *Um* G*-conjunto* X *é transitivo se ele possui uma única órbita, isto é, se para todos* $x, y \in X$, *existe* $g \in G$ *com* $gx = y$.

A seguir, definiremos uma construção de um grupo G que será muito útil no Capítulo 3, Subseção 3.2.2. Antes, precisamos da seguinte definição.

Definição 2.1.15. *Seja* K *um subgrupo (não necessariamente normal) de* G. *Então um subgrupo* Q *de* G *é dito um complemento de* K *em* G *se* $K \cap Q = \{e\}$ *e* $KQ = G$.

Definição 2.1.16. *Um grupo* G *é um produto semi-direto de* K *e* Q, *denotado por* $G = K \rtimes Q$, *se* $K \lhd G$ *e* K *tem um complemento* $Q_1 \simeq Q$. *Também dizemos que* G *decompõe-se sobre* K.

Exemplo 2.1.17. *(ROTMAN, 1995) Se* $D_n = \langle a, b\rangle$, *onde* $\langle a\rangle \simeq \mathbb{Z}_n$ *e* $\langle b\rangle \simeq \mathbb{Z}_2$, *tem-se* $\langle a\rangle \lhd D_n$ *e* $\langle b\rangle$ *é um complemento de* $\langle a\rangle$. *Logo,* $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$.

2.1.2 Anéis e Corpos

Definição 2.1.18. *Um* anel $(R, +, \cdot)$ *é um conjunto* R *composto por duas operações binárias, denotadas por* $+$ *e* $\cdot$*, tais que*

(i) R *é um grupo abelino com respeito a* $+$*.*

(ii) A operação $\cdot$ *é associativa, isto é, dados* $a, b, c \in R$*, vale*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(iii) A lei distributiva vale, isto é, para todos $a, b, c \in R$*, temos*

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ e } (b + c) \cdot a = b \cdot a + c \cdot a.$$

De agora em diante, adotaremos o símbolo 0 como elemento neutro da soma $(+)$ em R.

Definição 2.1.19. *(i) Um anel é dito um anel com identidade se o anel tem uma identidade multiplicativa, isto é, se existe um elemento* 1 *tal que* $a \cdot 1 = 1 \cdot a = a$*, para todo* $a \in R$*.*

(ii) Um anel é dito comutativo se $\cdot$ *é comutativa.*

(iii) Um anel é dito um domínio de integridade se ele é um anel comutativo com identidade $1 \neq 0$*, onde* $a \cdot b = 0$ *implica que* $a = 0$ *ou* $b = 0$*.*

(iv) Um anel é dito um anel de divisão se os elementos não nulos de R *formam um grupo sobre* $\cdot$*.*

(v) Um anel de divisão comutativo é denominado um corpo.

Definição 2.1.20. *Um subconjunto* S *de um anel* R *é denominado um subanel de* R *se* S *é fechado sob as operações* $+$ *e* $\cdot$ *de* R *e é um anel com estas operações.*

Como todo anel R é um grupo aditivo abeliano, então é natural estendermos a Definição 2.1.8 de homomorfismo de grupos para anéis. Sejam $(R, +, \cdot)$ e $(S, \oplus, *)$ dois anéis. Dados $a, b \in R$, uma aplicação $f : R \to S$ é um homomorfismo de anéis se

$$f(a + b) = f(a) \oplus f(b) \text{ e } f(a \cdot b) = f(a) * f(b).$$

Um isomorfismo é um homomorfismo bijetor e também denotaremos anéis R e S isomorfos como $R \simeq S$.

Definição 2.1.21. *Um subconjunto* J *de um anel* R *é dito um ideal se* J *é um subanel de* R *e, para todos* $a \in J$ *e* $r \in R$*, temos* $ar \in J$ *e* $ra \in J$*.*

Definição 2.1.22. *Seja R um anel. Um ideal J de R é dito principal se existe $a \in R$ tal que $\langle a \rangle = J$. Neste caso, J é também dito o ideal principal gerado por a.*

Se J é um ideal do anel R e $a \in R$, então a classe residual de a módulo J é o conjunto

$$a + J := \{a + c : c \in J\}. \tag{2.7}$$

Dados $a, b \in R$, podemos definir duas operações para o conjunto das classes residuais módulo J (por abuso de notação, utilizaremos os mesmos símbolos que descrevem as operações de R), a saber

$$(a + J) + (b + J) = (a + b) + J \quad \text{e} \quad (a \cdot J) \cdot (b \cdot J) = (a \cdot b) \cdot J. \tag{2.8}$$

Definição 2.1.23. *O anel das classes residuais do anel R módulo o ideal J sobre as operações dadas em (2.8) é dito o anel das classes residuais (ou anel quociente) de R módulo J e é denotado por R/J.*

O Exemplo 2.1.24 é uma versão levemente modificada do (LIDL, 1997, Theorem 1.38).

Exemplo 2.1.24. *(LIDL, 1997) Dados $\mathbb{Z}$ o anel dos números inteiros e p um número primo, o anel $\mathbb{Z}/\langle p \rangle$ das classes residuais dos inteiros módulo o ideal principal gerado por p é um corpo.*

Observação 2.1.25. *De agora em diante, denotaremos o corpo $\mathbb{Z}/\langle p \rangle$ como $\mathbb{F}_p$.*

Seja F um corpo qualquer. Defina o conjunto $F[x]$ formado por elementos da forma

$$f(x) = \sum_{i=0}^{n} f_i x^i,$$

onde os coeficientes $f_i \in F$, para todo $0 \leq i \leq n$, e $x \notin F$ é uma indeterminada sobre F. O número inteiro não negativo n é dito o grau de $f(x)$.

Dados dois polinômios $f(x) = \sum_{i=0}^{n} f_i x^i, g(x) = \sum_{i=0}^{m} g_i x^i \in F[x]$, onde $n \leq m$, defina as seguintes operações

$$f(x) + g(x) = \sum_{i=0}^{n} (f_i + g_i)\, x^i + \sum_{i=n+1}^{m} g_i x^i \text{ e} \tag{2.9}$$

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ onde } c_k = \sum_{i+j=k} a_i b_j. \tag{2.10}$$

De posse destas operações, verifica-se que $F[x]$ é um anel. Mais ainda

Teorema 2.1.26. *(LIDL, 1997) $F[x]$ é um domínio de ideais principais. De fato, para todo ideal $J \neq \langle 0 \rangle$ de $F[x]$, existe um polinômio mônico unicamente determinado $g(x) \in F[x]$ com $J = \langle g(x) \rangle$.*

Definição 2.1.27. *Um polinômio $f(x) \in F[x]$ é dito ser irredutível sobre F (ou irredutível em $F[x]$, ou primo em $F[x]$) se $f(x)$ tem grau positivo e $f(x) = g(x)h(x)$, $g(x), h(x) \in F[x]$, implica que ou $g(x)$, ou $h(x)$, é um polinômio constante.*

Teorema 2.1.28. *(LIDL, 1997) Para $f(x) \in F[x]$, o anel das classes residuais $F[x]/\langle f(x) \rangle$ é um corpo se, e somente se, $f(x)$ é irredutível sobre F.*

Definição 2.1.29. *Seja K um subcorpo de um corpo F e M qualquer subconjunto de F. Então o corpo $K(M)$ é definido como a interseção de todos os subcorpos de F contendo tanto K e M, e é dito a extensão (de corpo) de K obtida por adjuntar os elementos de M. Para $M = \{\theta_1, \theta_2, ..., \theta_n\}$ escrevemos $K(M) = K(\theta_1, \theta_2, ..., \theta_n)$. Se M consiste de um único elemento $\theta \in F$, então $L = K(\theta)$ é dito ser uma extensão simples de K, e θ é dito um elemento definidor de L sobre K.*

Definição 2.1.30. *Seja K um subcorpo de F e $\theta \in F$. Se θ satisfaz uma equação polinomial não trivial com coeficientes em K, isto é, se $a_n\theta^n + ... + a_1\theta + a_0 = 0$, com $a_i \in K$ não todos nulos, então θ é dito ser algébrico sobre K. Uma extensão L de K é dita algébrica sobre K (ou uma extensão algébrica de K) se todo elemento de L é algébrico sobre K.*

Definição 2.1.31. *Se $\theta \in F$ é algébrico sobre K, então o polinômio mônico unicamente determinado $g(x) \in K[x]$, gerador do ideal $J = \{f(x) \in K[x] : f(\theta) = 0\} \subset K[x]$, é dito o polinômio minimal (ou polinômio definidor, ou polinômio irredutível) de θ sobre K. Por grau de θ sobre K, queremos dizer o grau de $g(x)$.*

Definição 2.1.32. *Seja F uma extensão de corpo de K. Se F, considerado como um espaço vetorial sobre K, é de dimensão finita, então F é dito uma extensão finita de K. A dimensão do espaço vetorial F sobre K é então dita o grau de F sobre K, e será denotada por $[F : K]$.*

O resultado a seguir será usado constantemente neste trabalho, principalmente o item (i).

Teorema 2.1.33. *(LIDL, 1997) Seja $\theta \in F$ algébrico de grau n sobre K e $g(x)$ o polinômio minimal de θ sobre K. Então*

(i) $K(\theta)$ é isomorfo a $K[x]/\langle g(x) \rangle$.

(ii) $[K(\theta) : K] = n$ e $\{1, \theta, ..., \theta^{n-1}\}$ é uma base de $K(\theta)$ sobre K.

(iii) Todo $\alpha \in K(\theta)$ é algébrico sobre K e seu grau sobre K é um divisor de n.

De acordo com a proposta deste trabalho, de agora em diante consideraremos apenas corpos finitos. Os resultados apresentados a seguir descrevem a estrutura destes corpos.

Lema 2.1.34. *(LIDL, 1997) Seja F um corpo finito contendo um subcorpo K com q elementos. Então F tem q^m elementos, onde $m = [F : K]$.*

Teorema 2.1.35. *(LIDL, 1997) Seja F um corpo finito. Então F tem p^n elementos, onde o primo p é a característica de F e n é o grau de F sobre seu subcorpo primo.*

Lema 2.1.36. *(LIDL, 1997) Se F é um corpo finito com q elementos, então todo $a \in F$ satisfaz $a^q = a$.*

Um questionamento natural é se podemos construir um corpo finito com p^n elementos, para quaisquer p primo e n um inteiro positivo. O próximo teorema, conhecido como Teorema da Existência e Unicidade de Corpos Finitos, nos garante que não há restrições para tais números.

Teorema 2.1.37. *(LIDL, 1997) Para todo primo p e todo inteiro positivo n existe um corpo finito com p^n elementos. Qualquer corpo finito com $q = p^n$ elementos é isomorfo ao corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.*

Conforme a unicidade (a menos de isomorfismo) vista no Teorema 2.1.37, denotaremos todos os corpos finitos com q elementos como $\mathbb{F}_q$, onde $q = p^n$, para um primo p e n um inteiro positivo.

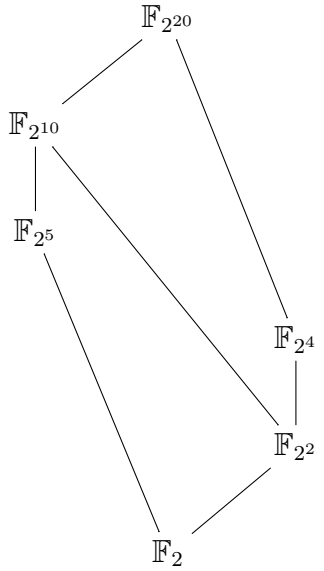
Teorema 2.1.38. *(LIDL, 1997) Seja $\mathbb{F}_q$ o corpo finito com $q = p^n$ elementos. Então todo subcorpo de $\mathbb{F}_q$ tem ordem p^m, onde m é um divisor positivo de n. Reciprocamente, se m é um divisor positivo de n, então existe exatamente um subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Teorema 2.1.39. *(LIDL, 1997) Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ dos elementos não nulos de $\mathbb{F}_q$ é cíclico.*

Definição 2.1.40. *Um gerador do grupo cíclico $\mathbb{F}_q^*$ é dito um* elemento primitivo *de $\mathbb{F}_q$.*

Definição 2.1.41. *Um polinômio $f(x) \in \mathbb{F}_q[x]$ de grau $m \geq 1$ é dito um* polinômio primitivo sobre $\mathbb{F}_q$ *se ele é o polinômio minimal sobre $\mathbb{F}_q$ de um elemento primitivo de $\mathbb{F}_{q^m}$.*

Exemplo 2.1.42. *O reticulado do corpo finito $\mathbb{F}_{2^{20}}$ e todos os seus subcorpos são representados pelo seguinte diagrama*



onde as linhas representam as relações de inclusão, que analagomante representam relações de divisibilidade, de acordo com o Teorema 2.1.38.

Teorema 2.1.43. *(LIDL, 1997) Seja $\mathbb{F}_q$ um corpo finito e $\mathbb{F}_r$ uma extensão de corpo finita de $\mathbb{F}_q$. Então $\mathbb{F}_r$ é uma extensão algébrica simples de $\mathbb{F}_q$ e todo elemento primitivo de $\mathbb{F}_r$ pode servir com um elemento definidor de $\mathbb{F}_r$ sobre $\mathbb{F}_q$.*

Corolário 2.1.44. *(LIDL, 1997) Para todo corpo finito $\mathbb{F}_q$ e todo inteiro positivo n existe um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n.*

Assim, de acordo com o Teorema 2.1.33 e o Corolário 2.1.44, para construirmos extensões de um corpo finito $\mathbb{F}_q$, basta encontrarmos um polinômio irredutível $f(x) \in \mathbb{F}_q[x]$ com grau compatível com o grau da extensão desejada, e considerarmos o anel quociente $\mathbb{F}_q[x]/\langle f(x)\rangle$.

Os Teoremas 2.1.33 e 2.1.37 (unicidade) afirmam que, dados $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível de grau n, e α uma raiz de $f(x)$, então

$$\mathbb{F}_{q^n} \simeq \mathbb{F}_q(\alpha) \simeq \mathbb{F}_q[x]/\langle f(x)\rangle, \tag{2.11}$$

ou seja, existem diferentes representações para o corpo finito de q^n elementos. Mais ainda, como todo corpo finito $\mathbb{F}_{q^n}$ pode ser interpretado como um $\mathbb{F}_q-$espaço vetorial de dimensão n, então, do ponto de vista de espaços vetoriais, temos

$$\mathbb{F}_{q^n} \simeq \mathbb{F}_q(\alpha) \simeq \mathbb{F}_q[x]/\langle f(x)\rangle \simeq \mathbb{F}_q^n, \tag{2.12}$$

e essas identificações serão utilizadas com frequência e livremente nos capítulos posteriores.

Para finalizarmos esta subseção, apresentamos um resultado que caracteriza todos os automorfismos de um corpo finito.

Teorema 2.1.45. *(LIDL, 1997) Os automorfismos distintos de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ são exatamente as aplicações $\sigma_0, \sigma_1, ..., \sigma_{n-1}$, definidas por $\sigma_i(\alpha) = \alpha^{q^i}$, para $\alpha \in \mathbb{F}_{q^n}$ e $0 \leq j \leq n-1$.*

Para $q = p$ primo, os automorfismos distintos dados no Teorema 2.1.45 formam um grupo conhecido como *Grupo de Galois* $Gal\left(\mathbb{F}_{q^n} : \mathbb{F}_q\right)$, onde $Gal\left(\mathbb{F}_{q^n} : \mathbb{F}_q\right) = \langle \sigma_1 \rangle$.

2.2 Códigos Corretores de Erros Clássicos

Códigos de subespaço podem ser interpretados como uma generalização dos códigos corretores de erros clássicos uma vez que, conforme será visto, cada palavra código de um código de subespaço pode ser interpretada como um código linear em $\mathbb{F}_q^n$. Além disso, como será visto no Capítulo 5, códigos corretores de erros serão úteis para a proposta de construção de redes transmissoras de informações quânticas. Por estas razões, nesta seção revisaremos os principais conceitos e alguns resultados sobre códigos lineares e, em particular, cíclicos, no contexto clássico. As principais referências desta seção são (BLAKE, 1975; HEFEZ, 2002; MACWILLIAMS, 1983).

Definição 2.2.1. *Seja A um conjunto finito qualquer provido de uma métrica. Um* código corretor de erros *$\mathcal{C}$ é um subconjunto de A^n, onde n é um inteiro positivo dito o comprimento do código. Os elementos de $\mathcal{C}$ são ditos* palavras código.

Dados $\mathcal{C}$ um código e duas palavras código $u = (u_1, u_2, ..., u_n)$ e $v = (v_1, v_2, ..., v_n)$, a distância de Hamming entre elas é definida como

$$d_H(u, v) := \left|\{i : u_i \neq v_i, 1 \leq i \leq n\}\right|. \tag{2.13}$$

O conjunto A^n equipado com a distância de Hamming é um espaço métrico. De fato, a distância de Hamming satisfaz as seguintes condições

Proposição 2.2.2. *(HEFEZ, 2002) Dados $u, v, w \in A^n$, valem as seguintes propriedades*

(i) $d_H(u, v) \geq 0$, *valendo a igualdade se, e somente se, $u = v$;*

(ii) $d_H(u, v) = d_H(v, u)$;

(iii) $d_H(u, v) \leq d_H(u, w) + d_H(w, v)$.

Seja $\mathcal{C} \subset A^n$ um código. A *distância mínima* de $\mathcal{C}$ é o número

$$d := \min\left\{d_H(u, v) : u, v \in \mathcal{C} \text{ e } u \neq v\right\}. \tag{2.14}$$

De agora em diante, assumiremos que $A = \mathbb{F}_q$, o corpo finito com q elementos, onde q é uma potência de primo. Logo $\mathbb{F}_q^n$ é um $\mathbb{F}_q-$espaço vetorial e $\mathcal{C} \subset \mathbb{F}_q^n$. O espaço métrico $\mathbb{F}_q^n$ com a métrica de Hamming $d_H(.,.)$ será chamado espaço de Hamming.

Definição 2.2.3. *Um código $\mathcal{C}$ é um código linear se $\mathcal{C}$ é um subespaço vetorial de $\mathbb{F}_q^n$. Assim um $(n,k,d)-$código linear $\mathcal{C}$ é um subespaço k dimensional de $\mathbb{F}_q^n$ com distância mínima d.*

Seja $B = \{v_1, v_2, ..., v_k\}$ uma base do $(n,k,d)-$código linear $\mathcal{C}$. Para todo $1 \leq i \leq k$, cada palavra código $v_i \in \mathcal{C}$ pode ser representada como $v_i = (v_{i1}, v_{i2}, ..., v_{in})_{\mathcal{B}}$, isto é, as coordenadas de v_i com relação a uma base $\mathcal{B}$ de $\mathbb{F}_q^n$. Logo, a matriz geradora do código $\mathcal{C}$ associada à base $\mathcal{B}$ é dada por

$$G := \begin{pmatrix} v_{11} & v_{12} & ... & v_{1n} \\ v_{21} & v_{22} & ... & v_{2n} \\ \vdots & \vdots & ... & \vdots \\ v_{k1} & v_{k2} & ... & v_{kn} \end{pmatrix}, \text{ tal que } \mathcal{C} = \left\{ xG : x \in \mathbb{F}_q^k \right\}.$$

Para toda matriz geradora G de um $(n,k,d)-$código linear $\mathcal{C}$, existe uma matriz H de ordem $(n-k) \times n$, também com entradas em $\mathbb{F}_q$, tal que

$$GH^T = 0_{k \times (n-k)}, \tag{2.15}$$

onde o superíndice T descreve a operação transposição de matrizes.

A matriz H dá origem ao código linear dual a $\mathcal{C}$ (MACWILLIAMS, 1983) e é dita a matriz verificação de paridade de $\mathcal{C}$. Ela desempenha um papel central no processo de decodificação de $\mathcal{C}$.

Exemplo 2.2.4. *Um código de Hamming binário corretor de um único erro $\mathcal{H}$ possui comprimento $n = 2^r - 1$ $(r \geq 2)$, e sua matriz verificação de paridade é formada por todos os vetores binários não nulos de comprimento r, cada um usado uma única vez. Logo, $\mathcal{H}$ é um $(2^r - 1, 2^r - 1 - r, 3)-$código linear.*

Definição 2.2.5. *Dados $a \in A^n$ e t um número inteiro não-negativo, os conjuntos*

$$D_t(a) := \{u \in A^n : d_H(u,a) \leq t\} \text{ e } E_t(a) := \{u \in A^n : d_H(u,a) = t\}, \tag{2.16}$$

são ditos o disco e a esfera de centro a e raio t, respectivamente.

Definição 2.2.6. *Sejam $\mathcal{C}$ um código com distância mínima d e $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$. O código $\mathcal{C}$ é dito perfeito se*

$$\bigcup_{c \in \mathcal{C}} D_\kappa(c) = \mathbb{F}_q^n.$$

Teorema 2.2.7. *(MACWILLIAMS, 1983) Os códigos de Hamming $\mathcal{H}$ do Exemplo 2.2.4 são perfeitos.*

Na verdade, de acordo com (MACWILLIAMS, 1983),

(i) Os $\left(\frac{q^m-1}{q-1}, n-m, 3\right)-$códigos de Hamming sobre $\mathbb{F}_q$,

(ii) o $(23, 12, 7)-$código de Golay binário $\mathcal{G}_{23}$ e

(iii) o $(11, 6, 5)-$código de Golay ternário $\mathcal{G}_{11}$

são perfeitos. As definições de códigos de Hamming e de Golay, além de suas propriedades, podem ser vistas em (MACWILLIAMS, 1983).

Teorema 2.2.8. *(MACWILLIAMS, 1983) Um código perfeito não trivial sobre qualquer corpo $\mathbb{F}_q$ deve ter os mesmos parâmetros n, k e d dos códigos de Hamming ou de Golay.*

2.2.1 Códigos Cíclicos

Definição 2.2.9. *Um código $\mathcal{C} \subset \mathbb{F}_q^n$ é dito um código cíclico se, para todo $(c_1, c_2, ..., c_n) \in \mathcal{C}$, então o vetor $(c_n, c_1, ..., c_{n-1}) \in \mathcal{C}$.*

O anel quociente $\mathcal{R}_{q,n} = \mathbb{F}_q[x]/\langle x^n - 1\rangle$ dos polinômios $f(x) = f_0 + f_1x + ... + f_{n-1}x^{n-1}$ admite a soma e o produto de polinômios módulo $x^n - 1$ usuais. Esta estrutura é dita semissimples se $\text{mdc}(q, n) = 1$ e, de agora em diante, sempre consideraremos $\mathcal{R}_{q,n}$ como um anel semissimples. Maiores considerações sobre esta condição podem ser verificadas em (BLAKE, 1975; MACWILLIAMS, 1983).

É de verificação direta que a aplicação

$$\begin{array}{rcl} \varphi : \mathbb{F}_q^n & \to & \mathcal{R}_{q,n} \\ (v_0, v_1, ..., v_{n-1}) & \mapsto & \sum_{i=0}^{n-1} v_i x^i \end{array} \tag{2.17}$$

é um isomorfismo de $\mathbb{F}_q$-espaços vetoriais. Assim, de acordo com a identificação (2.12) e a Definição 2.1.21, verifica-se que todo código cíclico $\mathcal{C}$ pode ser visto como um ideal de $\mathcal{R}_{q,n}$.

Teorema 2.2.10. *(MACWILLIAMS, 1983) Seja $\mathcal{C}$ um ideal em $\mathcal{R}_{q,n} = \mathbb{F}_q[x]/\langle x^n - 1\rangle$, isto é, um código cíclico de comprimento n.*

(i) Existe um único polinômio mônico $g(x)$ de grau mínimo em $\mathcal{C}$;

(ii) $\mathcal{C} = \langle g(x)\rangle$, isto é, $g(x)$ é um polinômio gerador de $\mathcal{C}$;

(iii) $g(x)$ é um fator de $x^n - 1$;

(iv) Qualquer $c(x) \in \mathcal{C}$ pode ser escrito unicamente como $c(x) = f(x)g(x)$ em $\mathbb{F}_q[x]$, onde $f(x) \in \mathbb{F}_q[x]$ tem grau menor que $n - r$, $r = \partial g(x)$. A dimensão de $\mathcal{C}$ é $n - r$. Assim a mensagem $f(x)$ torna-se a palavra código $f(x)g(x)$;

(v) Se $g(x) = g_0 + g_1x + \ldots + g_rx^r$, *então* $\mathcal{C}$ *é gerado* $\left($*como um subespaço de* $\mathbb{F}_q^n\right)$ *pelas linhas da matriz geradora*

$$\begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_r & \cdots & 0 \\ & g_0 & g_1 & \cdots & g_{r-1} & g_r & \\ & & & \vdots & & & \\ 0 & \cdots & & g_0 & g_1 & \cdots & g_r \end{pmatrix} = \begin{pmatrix} g(x) \\ x.g(x) \\ \vdots \\ x^{n-r-1}.g(x) \end{pmatrix}. \tag{2.18}$$

Exemplo 2.2.11. *De acordo com (MACWILLIAMS, 1983), o código de Hamming definido no Exemplo 2.2.4 é um código cíclico.*

2.3 Geometria Projetiva

Nesta seção, abordaremos, de forma bastante superficial, alguns conceitos e resultados das geometrias afim e projetiva, necessários para a definição de códigos de subespaço e o completo entendimento do Teorema Fundamental da Geometria Projetiva que, por sua vez, é primordial para a caracterização de todas as isometrias (simetrias) no espaço projetivo, que é exatamente o que se deseja para construção de códigos geometricamente uniformes neste contexto.

Durante toda esta seção, quando não for explicitado o contrário, V descreverá um K-espaço vetorial de dimensão n, em que n é um número inteiro positivo e K um corpo qualquer. Em particular, estaremos interessados quando $K = \mathbb{F}_q$, isto é, K é o corpo finito com $q = p^t$ elementos.

As principais referências desta seção são (BAER, 1952; ROTMAN, 1995; TRAUTMANN, 2013b).

2.3.1 Geometria Afim

Definição 2.3.1. *Se* V *é um espaço vetorial e* $y \in V$, *então uma translação por* y *é a aplicação* $t_y : V \to V$ *definida por*

$$t_y(v) = v + y, \tag{2.19}$$

para todo $v \in V$. *Vamos denotar por* $T(V)$ *o grupo de todas as translações com a operação de composição.*

Dado o espaço vetorial $V = \mathbb{F}_q^n$, seja $GL(\mathbb{F}_q)$ o grupo formado por todas as transformações lineares não singulares sobre $\mathbb{F}_q^n$. O grupo $GL(\mathbb{F}_q)$ é dito *grupo linear geral* e, em algumas bibliografias, também é denotado como $GL(q)$.

Fixada uma base B de $\mathbb{F}_q^n$, via o isomorfismo entre os grupos de transformações e matrizes não singulares, por abuso de notação, $GL(\mathbb{F}_q)$ também representará o grupo das matrizes não singulares de ordem n com entradas em $\mathbb{F}_q$.

Se K é um corpo de escalares qualquer, então denotaremos o grupo linear geral como $GL(V)$.

Teorema 2.3.2. *(ROTMAN, 1995)*

$$|GL(\mathbb{F}_q)| = (q^n - 1)(q^n - q)...\left(q^n - q^{n-1}\right). \tag{2.20}$$

Definição 2.3.3. *Se V é um espaço vetorial sobre K, então o grupo afim, denotado por $Aff(V)$, é o grupo (sob a operação de composição) de todas as aplicações $a : V \to V$, ditas afinidades, para as quais existem $y \in V$ e $g \in GL(V)$ tais que*

$$a(v) = gv + y, \tag{2.21}$$

para todo $v \in V$. É de verificação imediata que a é uma composição de t_y e g.

Dados quaisquer $v, y \in V$, para qualquer $g \in GL(V)$, tem-se

$$gt_y g^{-1}(v) = gt_y\left(g^{-1}v\right) = g\left(g^{-1}v + y\right) = v + gy = t_{gy}(v) \tag{2.22}$$

e, portanto, verifica-se que $T(V) \lhd Aff(V)$.

Definição 2.3.4. *Se S é um subespaço vetorial de dimensão m de um espaço vetorial V, então a classe lateral $W = S + v$, em que $v \in V$, é dita um $m-$subespaço afim de V. A dimensão de $S + v$ é definida como sendo a dimensão do subespaço S.*

Assim, por exemplo, se S_1 e S_2 são subespaços vetoriais de dimensão 1 e 2 de V, então dizemos que $W_1 = S_1 + v$ e $W_2 = S_2 + v$ são uma reta e um plano afins, respectivamente.

Definição 2.3.5. *Dado um espaço vetorial V, seja A um conjunto e, para $0 \leq m \leq n$, defina $L_m(A)$ como sendo uma família de subconjuntos de A (chamada de m-subespaços afins). Se $\alpha : V \to A$ é uma bijeção tal que um subconjunto W de V é um m-subespaço afim se, e somente se, $\alpha(W) \in L_m(A)$, então $(A, L_*(A), \alpha)$ é dito um n-espaço afim sobre K com espaço vetorial V associado.*

Quando não houver perigo de confusão, será implícito que o n-espaço afim $(A, L_*(A), \alpha)$ está associado ao espaço vetorial V.

Exemplo 2.3.6. *Se $A = V$ e $L_m(V) = \{S + v : S$ é um subespaço vetorial de dimensão m e $v \in V\}$, então $(V, L_*(V), Id)$, onde Id descreve a transformação linear identidade, é um espaço afim conhecido como espaço afim padrão de V sobre K.*

Definição 2.3.7. *Se $(A, L_*(A), \alpha)$ e $(B, L_*(B), \beta)$ são espaços afins sobre K, então uma bijeção $f : A \to B$ é um isomorfismo afim se, para todo $0 \leq m \leq n$, um subconjunto W de A pertence a $L_m(A)$ se, e somente se, $f(W)$ pertence a $L_m(B)$. Neste caso, dizemos que $(A, L_*(A), \alpha)$ e $(B, L_*(B), \beta)$ são espaços afins isomorfos.*

É de verificação direta que os espaços afins $(A, L_*(A), \alpha)$ e $(V, L_*(V), Id)$ são isomorfos, a partir do isomorfismo afim α. Logo, todo n-espaço afim é isomorfo ao n-espaço afim padrão.

Denotaremos por $Aut\,(A, L_*(A), \alpha)$ o grupo de todos os automorfismos afins de $(A, L_*(A), \alpha)$, cuja operação é a composição de automorfismos.

Teorema 2.3.8. *(ROTMAN, 1995) Se $(A, L_*(A), \alpha)$ é um espaço afim associado ao espaço vetorial V, então*

$$Aut\,(V, L_*(V), Id) \simeq Aut\,(A, L_*(A), \alpha)\,. \tag{2.23}$$

Mais ainda, dois espaços afins $(A, L_*(A), \alpha)$ e $(B, L_*(B), \beta)$ sobre K são isomorfos se, e somente se, eles possuem espaços vetoriais associados de mesma dimensão.

De posse do Teorema 2.3.8, denotaremos, a menos de isomorfismo, o grupo de automorfismos afins de V como $Aut(V)$. Verificamos que $Aff(V)$ é um subgrupo de $Aut(V)$ e, conforme veremos a seguir, para alguns casos particulares, tem-se que $Aff(V) = Aut(V)$.

O conceito de transformação semilinear exerce um papel fundamental neste trabalho, quando da caracterização de isometrias para códigos de subespaço.

Definição 2.3.9. *Sejam V e U espaços vetoriais sobre K. Uma aplicação $f : V \to U$ é uma transformação semilinear se existe $\sigma \in Aut(K)$, o grupo de automorfismos de K, tal que, para todos $x, y \in V$ e todo $\lambda \in K$, valem*

$$f(x+y) = f(x) + f(y) \text{ e} \tag{2.24}$$

$$f(\lambda x) = \sigma(\lambda) f(x). \tag{2.25}$$

Uma transformação semilinear f é não singular se a mesma é uma bijeção.

Transformações lineares entre espaços vetoriais são casos particulares de transformações semilineares. De fato, basta considerar $\sigma = Id$. Além disso, toda transformação semilinear não singular $f : V \to V$ é um automorfismo afim.

Para cada transformação semilinear não nula, é possível associar um único automorfismo do corpo K. Assim, dadas as transformações semilineares $f, g : V \to V$, com os respectivos automorfismos associados σ e τ, então a transformação semilinear composta $f \circ g$ possui o automorfismo associado $\sigma \circ \tau$ de K. Se f é não singular, então f^{-1} também é uma transformação semilinear não singular associada ao automorfismo σ^{-1} de K.

Definição 2.3.10. *Todas as transformações semilineares não singulares sobre um espaço vetorial V formam um grupo com a operação de composição de transformações. Este grupo é denotado por $\Gamma L(V)$ e dito o grupo semilinear geral.*

Assim, verifica-se

$$GL(V) < \Gamma L(V) \leq Aut(V). \tag{2.26}$$

O próximo teorema (Teorema 2.3.11) afirma que, na verdade, $\Gamma L(V) = Aut(V)$.

Teorema 2.3.11. *(ROTMAN, 1995) Se V e U são espaços vetoriais isomorfos de dimensão $n \geq 2$ sobre um corpo K, então todo isomorfismo afim $f : V \to U$ tem a forma $f = t_u g$, para algum $u \in U$ e alguma transformação semilinear não singular g, isto é, para todo $x \in V$,*

$$f(x) = g(x) + u. \tag{2.27}$$

Observação 2.3.12. *No Teorema 2.3.11 é necessário compor a transformação semilinear não singular g com uma translação para que possamos garantir a condição $f(0) = 0$, necessária para a prova deste resultado. Logo, a menos de uma translação, todo isomorfismo afim é uma transformação semilinear não singular.*

Corolário 2.3.13. *(ROTMAN, 1995) Sejam V e W espaços vetoriais sobre um corpo K com $dim(V) = dim(W) \geq 2$. Se $g : V \to W$ é uma aplicação aditiva para a qual $g(v) = \lambda_v v$, para todo $v \in V$, com $\lambda_v \in K$, então todos os λ_v são iguais e g é uma transformação escalar, isto é, $g(v) = \lambda v$.*

Teorema 2.3.14. *(ROTMAN, 1995) Se V é um espaço vetorial de dimensão n sobre um corpo K, então $\Gamma L(V)$ é um produto semi-direto de $GL(V)$ por $Aut(K)$. Se $K = \mathbb{F}_q = \mathbb{F}_{p^t}$, para p um número primo, então*

$$|\Gamma L(\mathbb{F}_q)| = t\,|GL(\mathbb{F}_q)|. \tag{2.28}$$

2.3.2 Teorema Fundamental da Geometria Projetiva

Assim como na Subseção 2.3.1, apesar dos próximos conceitos e resultados serem desenvolvidos para um contexto mais geral, é de nosso interesse que V seja um $\mathbb{F}_q$-espaço vetorial de dimensão n.

Dado o espaço vetorial V, consideremos o conjunto $V^* = V \setminus \{0\}$. Em tal conjunto, é possível definir a seguinte relação de equivalência $\sim$: $x \sim y$ se existe $\lambda \in K^*$ com $y = \lambda x$. A classe de equivalência de $x \in V^*$ será denotada por $[x]$.

Definição 2.3.15. *Se V é um espaço vetorial de dimensão $(n+1)$ sobre um corpo K, então $P(V) = \{[x] : x \in V^*\}$, é chamado n-espaço projetivo ou, simplesmente,* espaço projetivo. *Diz-se que $P(V)$ possui dimensão projetiva n.*

O conjunto $P(V)$ é um conjunto parcialmente ordenado a partir da inclusão de subespaços de V.

Definição 2.3.16. *Se W é um subconjunto de V, defina*

$$[W] = \{[x] : x \in W^*\} \subset P(V). \tag{2.29}$$

Se W é um subespaço vetorial de dimensão $(m+1)$ de V, então $[W]$ é dito um m-subespaço projetivo, cuja dimensão projetiva de $[W]$ é m.

De forma análoga como ocorre na geometria afim, alguns subespaços vetoriais de V recebem nomes especiais. Para $m = 0, 1, 2$ e $m = n-1$, os m-subespaços projetivos são conhecidos como pontos, retas, planos e hiperplanos projetivos, respectivamente.

Teorema 2.3.17. *(ROTMAN, 1995) Para cada $n \geq 0$ e $K = \mathbb{F}_q$*

$$|P(V)| = q^n + q^{n-1} + ... + q + 1. \tag{2.30}$$

Em particular, toda reta projetiva possui $q + 1$ pontos.

Após estas considerações, verifica-se que $P(V)$ pode ser visto como o conjunto de todos os subespaços de V $\left(\text{ou } \mathbb{F}_q^{n+1}\right)$.

Definição 2.3.18. *O subconjunto $\mathcal{G}_q(n+1, k)$, em que $0 \leq k \leq n+1$, formado por todos os subespaços $k-$dimensionais de V (ou $k-1$-subespaços projetivos de $P(V)$) é denominado* grassmanniana*, e assim*

$$P(V) = \bigcup_{i=0}^{n+1} \mathcal{G}_q(n+1, i). \tag{2.31}$$

O *coeficiente gaussiano* $\begin{bmatrix} n+1 \\ k \end{bmatrix}_q$ representa a quantidade de subespaços $k-$dimensionais de V ($k-1$-subespaços projetivos de $P(V)$), e é dado por

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^{n+1} - q^i}{q^k - q^i}, \tag{2.32}$$

onde vale a seguinte igualdade

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = \begin{bmatrix} n+1 \\ (n+1)-k \end{bmatrix}_q. \tag{2.33}$$

Definição 2.3.19. *Sejam V e U espaços vetoriais. Uma colineação (ou um isomorfismo projetivo) é uma bijeção $\theta : P(V) \to P(U)$, tal que um subconjunto S de $P(V)$ é um m-subespaço projetivo se, e somente se, $\theta(S)$ é um m-subespaço projetivo de $P(U)$. Dois espaços projetivos são isomorfos se existe uma colineação entre eles.*

Exemplo 2.3.20. *Dada $g : V \to U$ uma transformação semilinear não singular, então a função*

$$\begin{array}{rccc} P(g): & P(V) & \to & P(U) \\ & [x] & \mapsto & [g(x)], \end{array} \tag{2.34}$$

é uma colineação. Em particular, quando g for uma transformação linear, então diremos que $P(g)$ é uma projetividade.

Teorema 2.3.21. *(ROTMAN, 1995) Dois espaços projetivos $P(V)$ e $P(U)$ são isomorfos se, e somente se, $dim(V) = dim(U)$.*

O próximo teorema revela como é possível identificar um espaço afim imerso em um espaço projetivo.

Teorema 2.3.22. *(ROTMAN, 1995) Se $[W]$ é um hiperplano projetivo em um n-espaço projetivo $P(V)$ e se $x \in V \setminus W$, então à $A = P(V) \setminus [W]$ pode ser dada a estrutura de um n-espaço afim $(A, L_*(A), \alpha)$ com espaço vetorial associado W, onde $\alpha : W \to A$ é definido por $\alpha(w) = [w + x]$, para todo $w \in W$.*

A seguir, apresentaremos o Teorema Fundamental da Geometria Projetiva, ou Primeiro Teorema Fundamental da Geometria Projetiva (BAER, 1952, pag. 44), que desempenhará um papel central na classificação das isometrias em $P(V)$. Tais aplicações são essenciais para a proposta deste trabalho de caracterização dos códigos de subespaço geometricamente uniformes.

Teorema 2.3.23. *(ROTMAN, 1995)[Teorema Fundamental da Geometria Projetiva] Se V e U são espaços vetoriais isomorfos sobre um corpo K de dimensão $n + 1 \geq 3$, então cada colineação $f : P(V) \to P(U)$ tem a forma $f = P(g)$ para alguma transformação semilinear $g : V \to U$.*

Observação 2.3.24. *O grupo de todas as transformações escalares (Corolário 2.3.13) sobre V será denotado por $Z(V)$. Logo*

Teorema 2.3.25. *(ROTMAN, 1995) Se $dim(V) \geq 3$, o grupo $\Gamma L(V)/Z(V)$ é isomorfo ao grupo $Col(V)$ de todas as colineações de $P(V)$ com ele próprio. Se $dim(V) = 2$, então $\Gamma L(V)/Z(V)$ é isomorfo a um subgrupo do grupo de simetrias de $P(V)$.*

De posse dos Teoremas 2.3.14 e 2.3.25, apresentamos uma releitura do Teorema Fundamental da Geometria Projetiva para o caso de auto colineações

Teorema 2.3.26. *(TRAUTMANN, 2013b) Cada bijeção que preserva ordem (com respeito à relação de subconjunto), ou seja, toda colineação $f : P(V) \to P(V)$, onde $n \geq 2$, dado que $P(V)$ é um n-espaço projetivo, é induzida por uma transformação semilinear*

$$(A, \varphi) \in P\Gamma L(V) := GL(V)/Z(V) \rtimes Aut(K). \tag{2.35}$$

Observação 2.3.27. *Todo elemento de $Z(V)$ age como uma identidade projetiva em $P(V)$.*

De agora em diante, o grupo $P\Gamma L(V)$ será dito *grupo semilinear projetivo*, e o subgrupo $GL(V)/Z(V)$ será denotado por $PGL(V)$, e dito grupo linear projetivo. Durante todo este trabalho, assumiremos que o corpo de escalares do espaço vetorial V é $K = \mathbb{F}_q$. Logo, denotaremos os grupos semilinear e linear projetivos como $P\Gamma L(\mathbb{F}_q)$ e $PGL(\mathbb{F}_q)$, respectivamente.

3 Códigos de Subespaço

Neste capítulo, apresentamos a definição e vários resultados relacionados a códigos de subespaço, que são códigos eficientes para combater os erros e apagamentos que podem surgir durante as transmissões de pacotes de informações em redes *multicast*, dado o modelo de canal proposto no trabalho seminal (KöTTER, 2008). Existem diversas classes de códigos de subespaço, mas este capítulo é destinado à classe dos códigos de órbita.

Na Seção 3.1, apresentamos o modelo de canal proposto por Kötter e Kschischang para redes lineares aleatórias, a partir do fato de que a codificação desenvolvida pelos nós intermediários destas redes preserva espaços vetoriais, e que nem as fontes e nem os destinatários possuem informações sobre as características desses canais abstratos. Trata-se de um modelo atual e amplamente estudado.

Na Seção 3.2, definimos o espaço ambiente onde os códigos de subespaço estão imersos e as principais métricas utilizadas neste contexto. Definido o espaço métrico, apresentamos a definição de códigos de subespaço e, em particular, de códigos de subespaço de dimensão constante, além de limitantes inferiores e superiores para a cardinalidade desses códigos. Na Subseção 3.2.2, definimos a classe de códigos de dimensão constante conhecida como códigos de órbita. Estes códigos desempenharão um papel fundamental na caracterização de códigos geometricamente uniformes em $\mathcal{G}_q(n,k)$. Diversos resultados relativos à construção, cardinalidade e distância mínima destes códigos são apresentados.

3.1 Canal de Kötter e Kschischang e Codificação de Redes Aleatórias

Dada uma rede linear aleatória *multicast*, a cada *round*, os pacotes de informações enviados pela fonte são encaminhados para os primeiros nós intermediários, que codificam essas informações como combinações lineares, de forma aleatória, encaminhando tais combinações para os próximos nós intermediários, de forma que, no final deste processo, os destinatários buscam reverter tais combinações lineares aleatórias e recuperar as informações originalmente enviadas pelas fontes.

Como cada nó intermediário tem a capacidade de processar os pacotes de informações e repassá-los para o(s) próximo(s) nó(s), então qualquer interferência em uma única operação realizada por um nó, por exemplo, a partir de informação adicional (erro), ou do apagamento de um bloco de informação, pode comprometer toda a comunicação. Assim, nesta seção, estudaremos o modelo de canal considerado por Kötter e Kschischang e uma proposta para corrigir tais distorções. A referência desta seção é (KöTTER, 2008).

Assim como foi descrito em (KöTTER, 2008), e de acordo com as referências lá citadas, vamos considerar apenas o caso de codificação de rede aleatória *unicast*, ou seja, existem apenas um transmissor (ou fonte) e um destinatário. A expansão para o caso *multicast* é direta.

Suponhamos que a cada *round*, o transmissor envie ao destinatário as M informações $B = \{p_1, p_2, ..., p_M\} \subset \mathbb{F}_q^n$. A cada nó da rede que as informações de B atingem, estas estão sujeitas à $\mathbb{F}_q$-combinações lineares, além de erros introduzidos pela rede, de forma que, no final da transmissão, o destinatário colecionará uma quantidade L de novos vetores de $\mathbb{F}_q^n$, isto é, $\overline{B} = \{\overline{p}_1, \overline{p}_2, ..., \overline{p}_L\}$, tal que

$$\overline{p}_j = \sum_{i=1}^{M} h_{j,i} p_i + \sum_{t=1}^{T} g_{j,t} e_t, \text{ para cada } 1 \leq j \leq L, \tag{3.1}$$

onde $h_{j,i}, g_{j,t} \in \mathbb{F}_q$ e $e_t \in \mathbb{F}_q^n$. No caso em que a rede é livre de erros, então $e_t = \mathbf{0}$, para todo $1 \leq t \leq T$, em que $\mathbf{0}$ é o vetor nulo em $\mathbb{F}_q^n$.

O canal/rede que descreve a situação *unicast* (3.1) pode ser representado matricialmente como

$$\overline{P} = HP + GE, \tag{3.2}$$

onde $H \in M_{L\times M}(\mathbb{F}_q)$ e $G \in M_{L\times T}(\mathbb{F}_q)$ representam matrizes aleatórias que descrevem as diversas $\mathbb{F}_q$-combinações lineares realizadas nos nós intermediários da rede, $P \in M_{M\times n}(\mathbb{F}_q)$, $\overline{P} \in M_{L\times n}(\mathbb{F}_q)$ e $E \in M_{T\times n}(\mathbb{F}_q)$ representam as matrizes

$$P = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_M \end{pmatrix}, \overline{P} = \begin{pmatrix} \overline{p}_1 \\ \overline{p}_2 \\ \vdots \\ \overline{p}_L \end{pmatrix} \text{ e } \overline{E} = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_T \end{pmatrix}, \tag{3.3}$$

respectivamente.

Para o canal (3.2), desconsiderando o erro representado pela matriz E, verifica-se que o espaço vetorial gerado pelas linhas da matriz HP, que denotaremos por $rs(HP)$, é um subespaço vetorial do espaço vetorial gerado pelas linhas de P, ou seja, $rs(P)$. A situação em que $rs(HP)$ é um subespaço próprio de $rs(P)$ ocorre quando há um apagamento de posto ou um *min-cut* insuficiente. Portanto, o problema de transferência de pacotes de informações injetados pela fonte em uma rede pode ser interpretado como um problema de transferência de espaços vetoriais, gerados por tais sequências de informações.

Observação 3.1.1. *De agora em diante, dado V um $\mathbb{F}_q$-espaço vetorial de dimensão n, denotaremos a coleção de todos os subespaços de V (ou o $n-1$ espaço projetivo - Definição 2.3.15) por $\mathcal{P}_q(n)$, de acordo com a notação proposta por vários trabalhos que são base deste.*

Em (KöTTER, 2008), os autores definiram o operador $H_k(V)$, dito operador apagamento, que atua sobre $\mathcal{P}_q(n)$ da seguinte forma: Dada a palavra $W \in \mathcal{P}_q(V)$, com $dim(W) > k$, tem-se

$$H_k(W) := \begin{cases} W_1, & \text{subespaço de dimensão } k \text{ de } W, \text{ obtido de forma aleatória, ou} \\ W. \end{cases} \tag{3.4}$$

Observação 3.1.2. *Dadas as palavras $U, W, E \in \mathcal{P}_q(n)$, é possível descrever $U = H_k(W) \oplus E$, considerando que $dim(U \cap W) = k$ e $H_k(W) = U \cap W$.*

Definição 3.1.3. *(KöTTER, 2008) Um canal operador C associado com o espaço ambiente V é um canal com alfabeto de entrada e saída $\mathcal{P}_q(n)$. Como descrito na Observação 3.1.2, a entrada do canal W e a saída do canal U podem sempre ser relacionadas como*

$$U = H_k(W) \oplus E, \tag{3.5}$$

onde $dim(U \cap W) = k$ e E é um subespaço vetorial que representa os possíveis erros. Na transformação de W para U, dizemos que o canal operador comete $\rho = dim(W) - k$ apagamentos e $t = dim(E)$ erros.

Para encerrarmos esta seção, observa-se que à transmissão de palavras no contexto de codificação de redes corresponde à transmissão de “códigos lineares"no contexto da teoria da informação clássica.

Na próxima seção, descreveremos como construir códigos que corrigem os erros e apagamentos apontados na Definição 3.1.3.

3.2 Códigos de Subespaço

Nesta seção, apresentaremos duas métricas para o conjunto $\mathcal{P}_q(n)$, de forma que este possa ser visto como um espaço métrico. A partir desta constatação, definimos códigos de subespaço e, em particular, códigos (de subespaço) de dimensão constante. Derivamos alguns limitantes relacionados à cardinalidade de tais códigos, além de exibir alguns métodos de decodificação. Por fim, apresentamos duas definições e diversos resultados relacionados aos códigos de órbita, que desempenham um papel central neste trabalho.

As principais referências para esta seção são (ETZION, 2011; KHALEGHI D. SILVA, 2009; KöTTER, 2008; G.-LUERSSEN K. MORRISON, 2015; SILVA, 2008; TRAUTMANN, 2013a; TRAUTMANN F. MANGANIELLO, 2013).

3.2.1 Correção e Deteção de Erros

Para falarmos em códigos corretores de erros e/ou apagamentos em $\mathcal{P}_q(n)$, se faz necessário a definição de uma métrica neste contexto. O Lema 3.2.1 apresenta a primeira métrica definida em $\mathcal{P}_q(n)$.

Lema 3.2.1. *(KöTTER, 2008) A função $d : \mathcal{P}_q(n) \times \mathcal{P}_q(n) \to \mathbb{Z}_+$ dada por*

$$\begin{aligned} d_S(U,V) &:= dim(U) + dim(V) - 2dim(U \cap V) \\ &= dim(U+V) - dim(U \cap V), \end{aligned} \tag{3.6}$$

é uma métrica para $\mathcal{P}_q(n)$.

A métrica apresentada no Lema 3.2.1 é conhecida como *distância de subespaço*.

Em (SILVA, 2008), uma outra métrica para o espaço projetivo foi introduzida. Tal métrica é conhecida como a métrica da injeção onde, dados dois subespaços $U, V \in \mathcal{P}_q(n)$, temos

$$d_I(U,V) := \max\{dim(U), dim(V)\} - dim(U \cap V). \tag{3.7}$$

As métricas de subespaço e da injeção se relacionam da seguinte forma

$$d_I(U,V) = \frac{1}{2} d_S(U,V) + \frac{1}{2} \left| dim(V) - dim(U) \right|, \text{ para todos } U, V \in \mathcal{P}_q(n). \tag{3.8}$$

Em particular, se $U, V \in \mathcal{G}_q(n,k)$, então $2d_I(U,V) = d_S(U,V)$.

Existe uma terceira métrica utilizada no contexto de codificação de redes conhecida como a métrica do posto. Tal métrica não será utilizada em nenhum momento neste trabalho; para mais informações sobre esta e as demais métricas aqui citadas, indicamos as referências (GABIDULIN, 1985; KHALEGHI D. SILVA, 2009).

Observação 3.2.2. *De agora em diante, utilizaremos apenas a métrica de subespaço para descrever a distância entre dois subespaços do espaço projetivo $\mathcal{P}_q(n)$.*

Conforme foi observado em (KöTTER, 2008), a métrica de subespaço equivale a uma geodésica (caminho mais curto) no grafo de Hasse, que representa o reticulado dos subespaços de $\mathbb{F}_q^n$ ordenados parcialmente pela inclusão. Logo, os elementos de $\mathcal{P}_q(n)$ são os vértices deste grafo, e dois vértices U, V são unidos por uma aresta se, e somente se, $U \subset V$, ou $V \subset U$, e $|dim(U) - dim(V)| = 1$. O grafo de Hasse representa para o espaço métrico $(\mathcal{P}_q(n), d_S)$ o que o hipercubo representa para o espaço métrico de Hamming $\left(\mathbb{F}_q^n, d_H\right)$, utilizado na teoria de codificação clássica.

Em particular, se os vértices agora são compostos apenas por elementos de uma grassmanniana $\mathcal{G}_q(n,k)$, para algum $0 \leq k \leq n$, então este novo grafo é conhecido como grafo de Grassmann.

Exemplo 3.2.3. *Dado* $\mathbb{F}_2^3 = \{000, 100, 010, 001, 110, 011, 101, 111\}$*, o correspondente grafo de Hasse de* $\mathcal{P}_2(3)$ *é representado a partir das relações de inclusão descritas na Figura 5. Lá é fácil observar, por exemplo, que* $d_S\left(\langle 100\rangle, \mathbb{F}_2^3\right) = 2$*.*

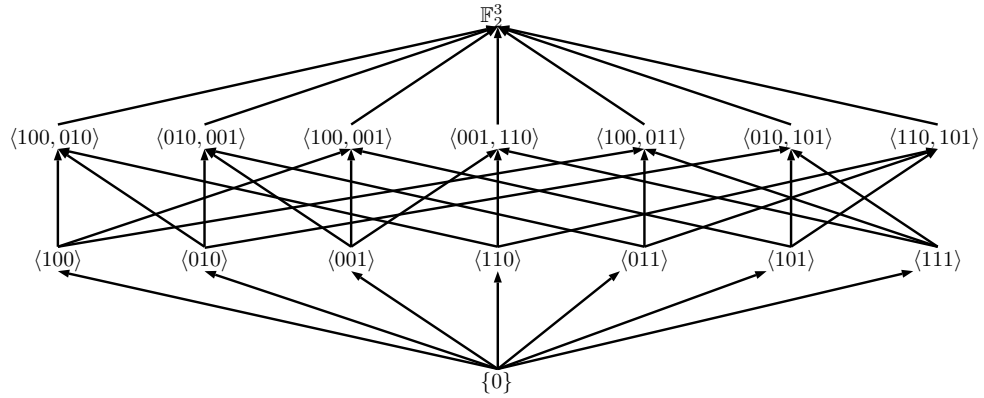


Figura 5 – Grafo de Hasse de $\mathbb{F}_2^3$

Definição 3.2.4. *Um* $(n, M, d)-$código de subespaço C *é uma coleção de* M *subespaços vetoriais de* $\mathbb{F}_q^n$ *com distância mínima* d*, calculada como* $d = \min_{U,V \in C : U \neq V} d_S(U, V)$*. Em particular, se todas as palavras código em* C *têm a mesma dimensão* k*, então* C *é um* $(n, M, d, k)-$*código de subespaço de dimensão constante, ou simplesmente um* código de dimensão constante*.*

Neste capítulo, consideraremos, prioritariamente, códigos de dimensão constante.

Observação 3.2.5. *Em particular, se* $C \subseteq \mathcal{G}_q(n, k)$ *é um código de dimensão constante então, para quaisquer* $U, V \in C$*, verificamos*

$$\begin{aligned} d_S(V, W) &= dim(U) + dim(V) - 2dim(U \cap V) \\ &= 2k - 2dim(U \cap V) \\ &= 2[k - dim(U \cap V)] \\ &= 2[dim(U + V) - k], \end{aligned} \tag{3.9}$$

uma vez que $dim(U + V) = dim(U) + dim(V) - dim(U \cap V)$*. Assim, a distância mínima de códigos de dimensão constante é sempre um número par, e*

$$d = d_S(C) \leq \min\{2k, 2(n - k)\}. \tag{3.10}$$

Fixada uma base $B = \{b_1, b_2, ..., b_n\}$ de $\mathbb{F}_q^n$, as coordenadas de cada vetor $v \in \mathbb{F}_q^n$ podem ser representadas em função de B, isto é, se $v = \sum_{i=1}^{n} v_i b_i$, então $v = (v_1, v_2, .., v_n)_B$. Assim, dados dois vetores $v = (v_1, v_2, .., v_n)_B$ e $u = (u_1, u_2, .., u_n)_B$, o produto interno usual é definido como

$$\langle v, u\rangle = \sum_{i=1}^{n} v_i u_i. \tag{3.11}$$

Se V é um subespaço k dimensional de $\mathbb{F}_q^n$, então o complemento ortogonal de V, denotado por $V^\perp$, é o subespaço $n-k$ dimensional

$$V^\perp := \left\{ u \in \mathbb{F}_q^n : \langle v, u \rangle = 0, \text{ para todo } v \in V \right\}. \tag{3.12}$$

Como observado em (KöTTER, 2008), dados $U, V \in \mathcal{P}_q(n)$, temos

$$\begin{aligned} d_S\left(U^\perp, V^\perp\right) &= dim\left(U^\perp + V^\perp\right) - dim\left(U^\perp \cap V^\perp\right) \\ &= dim\left[(U \cap V)^\perp\right] - dim\left[(U+V)^\perp\right] \\ &= [n - dim\,(U \cap V)] - [n - dim\,(U+V)] \\ &= dim(U+V) - dim(U \cap V) \\ &= d_S(U,V). \end{aligned}$$

uma vez que $(U+V)^\perp = U^\perp \cap V^\perp$ e $(U \cap V)^\perp = U^\perp + V^\perp$.

Definição 3.2.6. *Dado $C \subset \mathcal{P}_q(n)$ um (n, M, d)-código de subespaço, o código complementar correspondente a C é o $(n, M, d)-$código $C^\perp = \left\{V^\perp : V \in C\right\}$. Em particular, se $C \subset \mathcal{G}_q(n,k)$, então $C^\perp \subset \mathcal{G}_q(n, n-k)$.*

Observação 3.2.7. *De posse da definição de códigos complementares, quando considerarmos códigos de dimensão constante, assumiremos $k \leq \left\lfloor \frac{n}{2} \right\rfloor$.*

Definição 3.2.8. *Dado $V \in \mathcal{P}_q(n)$, a esfera de raio t centrada no subespaço V é definida como*

$$E_q(V,t) := \{U \in \mathcal{P}_q(n) : d_S(U,V) \leq t\}. \tag{3.13}$$

Teorema 3.2.9. *(ETZION, 2011) Para todo $V \in \mathcal{P}_q(n)$ com dimensão k, temos*

$$|E_q(V,t)| = \sum_{j=0}^{t} \sum_{i=0}^{j} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} n-k \\ j-i \end{bmatrix}_q q^{i(j-i)}. \tag{3.14}$$

Definição 3.2.10. *Dado $V \in \mathcal{G}_q(n,k)$, a esfera de raio t centrada no subespaço V e contida em $\mathcal{G}_q(n,k)$ é definida como*

$$E_q(V,k,t) := \{U \in \mathcal{G}_q(n,k) : d_S(U,V) \leq 2t\}. \tag{3.15}$$

Teorema 3.2.11. *(KöTTER, 2008) O número de subespaços em $E_q(V,k,t)$ é independente de V e igual a*

$$|E_q(V,k,t)| = |E_q(V,t) \cap \mathcal{G}_q(n,k)| = \sum_{i=0}^{t} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} n-k \\ i \end{bmatrix}_q, \tag{3.16}$$

para $t \leq k$.

Um código e-perfeito C é aquele que cobre e empacota todo o espaço ambiente, a partir de esferas de raio e centradas nas palavras código de C. Por códigos perfeitos triviais em $\mathcal{G}_q(n,k)$, entendemos o código 0-perfeito, que é todo o espaço ambiente, e o código n-perfeito, formado por uma única palavra código $V \in \mathcal{G}_q(n,k)$. Se considerarmos $\mathcal{P}_q(n)$ como espaço ambiente, então além dos códigos triviais definidos em $\mathcal{G}_q(n,k)$, existe uma terceira construção de código perfeito trivial. Para $n = 2m+1$ um número ímpar, o código formado pelas palavras código $\{0\}$ e $\mathbb{F}_q^n$ é m-perfeito.

Ao contrário do que ocorre no espaço de Hamming, temos os seguintes resultados

Teorema 3.2.12. *(MARTIN, 1995) Para quaisquer n, q e k, não existem códigos perfeitos não triviais em $\mathcal{G}_q(n,k)$.*

Posteriormente, em 2011, o Teorema 3.2.12 foi estendido para o caso geral, isto é,

Teorema 3.2.13. *(ETZION, 2011) Para quaisquer n e q, não existem códigos perfeitos não triviais em $\mathcal{P}_q(n)$.*

Em analogia aos limitantes clássicos para à cardinalidade dos códigos obtidos no espaço de Hamming, apresentaremos alguns resultados relativos à cardinalidade dos códigos de dimensão constante. O primeiro resultado é o bem conhecido *Limitante de Empacotamento e Cobertura de Esferas.*

Teorema 3.2.14. *(KöTTER, 2008) Sejam $C \subset \mathcal{G}_q(n,k)$ um $(n,|C|,d,k)$-código de dimensão constante e $E_q(V,k,t)$ a esfera de raio t centrada no subespaço $V \in \mathcal{G}_q(n,k)$, tal que $d \geq 2t$ e $s = \left\lfloor \dfrac{t-1}{2} \right\rfloor$. O tamanho do código C deve satisfazer*

$$\begin{aligned} |C| &\leq \frac{|\mathcal{G}_q(n,k)|}{|E_q(V,k,t)|} = \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{|E_q(V,k,t)|} < \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{q^{s^2} \begin{bmatrix} k \\ s \end{bmatrix}_q \begin{bmatrix} n-k \\ s \end{bmatrix}_q} \\ &< 4q^{(k-s)(n-s-k)}. \end{aligned}$$

Reciprocamente, existe um $(n,|C'|,k,d)$-código de dimensão constante C' com $d \geq 2t$, tal que $|C'|$ é limitada inferiormente por

$$\begin{aligned} |C'| &\geq \frac{|\mathcal{G}_q(n,k)|}{|E_q(V,k,t-1)|} = \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{|E_q(V,k,t-1)|} > \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{(t-1)q^{(t-1)^2} \begin{bmatrix} k \\ t \end{bmatrix}_q \begin{bmatrix} n-k \\ t-1 \end{bmatrix}_q} \\ &> \frac{1}{16t} q^{(k-t+1)(n-t-k+1)}. \end{aligned}$$

O próximo limitante superior para a cardinalidade de um código de dimensão constante C é análogo ao clássico *Limitante de Singleton*.

Teorema 3.2.15. *(KöTTER, 2008) Um $(n, |C|, k, d)-$código de dimensão constante C deve satisfazer*

$$|C| \leq \begin{bmatrix} n - \frac{(d-2)}{2} \\ \max\{k, n-k\} \end{bmatrix}_q . \tag{3.17}$$

Seja $\mathcal{A}_q(n, d, k)$ a cardinalidade máxima de um código de dimensão constante k com parâmetros n, q e $d = 2t$. Em (ETZION, 2011), os autores apresentam refinamentos de limitantes superiores para a cardinalidade dos códigos de dimensão constante em relação aos limitantes explicitados nos Teoremas 3.2.14 e 3.2.15. Apresentaremos apenas dois limitantes superiores. Para uma consulta sobre os demais limitantes, inclusive para o número $\mathcal{A}_q(n, d)$, que corresponde à cardinalidade máxima de $(n, M, d)-$códigos $C \subset \mathcal{P}_q(n)$, indicamos (ETZION, 2013; ETZION, 2011).

Teorema 3.2.16. *(ETZION, 2011)*

$$\mathcal{A}_q(n, d = 2t, k) \leq \prod_{i=0}^{k-t} \frac{q^{n-i} - 1}{q^{k-i} - 1}. \tag{3.18}$$

Teorema 3.2.17. *(ETZION, 2011)*

$$\mathcal{A}_q(n, d = 2t, k) \leq \left\lfloor \frac{q^n - 1}{q^k - 1} \left\lfloor \frac{q^{n-1} - 1}{q^{k-1} - 1} \ldots \left\lfloor \frac{q^{n-k+t} - 1}{q^t - 1} \right\rfloor \ldots \right\rfloor \right\rfloor . \tag{3.19}$$

É de verificação direta que o Teorema 3.2.17 é sempre mais refinado ou igual ao Teorema 3.2.16.

Definição 3.2.18. *Um código $C \subset \mathcal{G}_q(n, k)$ é dito ótimo se ele atinge qualquer limitante superior para a cardinalidade de códigos de dimensão constante, isto é,*

$$|C| = \mathcal{A}_q(n, d, k). \tag{3.20}$$

A seguir, abordaremos alguns métodos de decodificação para códigos de subespaço, que foram descritos em (TRAUTMANN, 2013a).

Definição 3.2.19. *Seja $C \subset \mathcal{P}_q(n)$ um código de subespaço e $R \in \mathcal{P}_q(n)$ uma palavra recebida*

(i) Um decodificador de máxima verossimilhança decodifica R como uma palavra código $U \in C$ que maximiza a probabilidade $P(R \text{ recebida} \mid U \text{ enviada})$, para todo $U \in C$.

(ii) Um decodificador de distância mínima escolhe a palavra código mais próxima à palavra recebida com respeito a distância mínima adotada (subespaço ou injeção). Se existe mais que uma palavra código que esteja mais próxima à palavra recebida, então o decodificador retorna "erro".

Como ocorre na teoria da informação clássica, temos o seguinte resultado.

Lema 3.2.20. *(TRAUTMANN, 2013a) Assuma que a distância mínima (subespaço ou injeção) de um código de subespaço $C \subset \mathcal{P}_q(n)$ é d, e seja $R \in \mathcal{P}_q(n)$ uma palavra recebida. Se existe $U \in C$ tal que a distância de R é, no máximo, $\left\lfloor \frac{(d-1)}{2} \right\rfloor$, então U é a única palavra mais próxima e o decodificador de distância mínima sempre decodificará R como U.*

O próximo método de decodificação é conhecido como “decodificação de lista", e também foi inspirado a partir do respectivo decodificador para códigos no espaço de Hamming.

Definição 3.2.21. *Dados um código de subespaço $C \subset \mathcal{P}_q(n)$ e uma palavra recebida $R \in \mathcal{P}_q(n)$, um decodificador de lista com limitante de erro t apresenta uma lista de palavras código $U_1, U_2, ..., U_m \in C$ cuja distância (subespaço ou injeção) de R é de, no máximo, t. Em outras palavras, tal lista de palavras código é igual ao conjunto $E_q(R,t) \cap C$.*

Se $C \subset \mathcal{G}_q(n,k)$, então um decodificador de lista com limitante de erro t apresenta uma lista igual ao conjunto $E_q(R,k,t) \cap C$.

3.2.2 Códigos de Órbita

Esta subseção é essencial para a proposta de caracterização de códigos de subespaço geometricamente uniformes. Definiremos e descreveremos os principais resultados sobre códigos de órbita, inicialmente apresentados em (TRAUTMANN F. MANGANIELLO, 2010). Em particular, o nosso interesse é focado na classe dos códigos de órbita cíclicos, uma vez que tais códigos podem ser vistos como blocos para construções mais gerais.

Devido ao $\mathbb{F}_q$-isomorfismo entre os espaços vetoriais $\mathbb{F}_q^n$ e $\mathbb{F}_{q^n}$ (Equação (2.12)), duas representações diferentes para os códigos de órbita cíclicos serão apresentadas. A única diferença entre tais representações é a forma de explicitar os elementos; utilizaremos aquela que for mais adequada para a situação proposta.

Por fim, apresentamos a definição de códigos de subespaço cíclicos, que podem ser vistos como uma união de códigos de órbita cíclicos, além de uma construção mais geral de códigos de órbita, novamente, fazendo uso dos códigos de órbita cíclicos.

As principais referências desta Subseção são (BARDESTANI, 2015; G.-LUERSSEN K. MORRISON, 2015; TRAUTMANN F. MANGANIELLO, 2013).

Iniciamos com a abordagem descrita em (TRAUTMANN F. MANGANIELLO, 2013).

Seja $V \in \mathcal{G}_q(n,k)$ um subespaço vetorial de $\mathbb{F}_q^n$. Podemos representar V como

$$V = rs(\mathcal{V}) = \left\{ x\mathcal{V} : x \in \mathbb{F}_q^k \right\}, \tag{3.21}$$

em que a sigla rs denota o espaço vetorial gerado pelas linhas de $\mathcal{V} \in M_{k\times n}(\mathbb{F}_q)$, e que diremos apenas espaço linha. A representação de V como $rs(\mathcal{V})$ não é única, uma vez que existe $\overline{\mathcal{V}} \neq \mathcal{V}$, tal que $rs(\overline{\mathcal{V}}) = V$. Como um simples exemplo, o espaço linha das matrizes $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \in M_{3\times 3}(\mathbb{F}_2)$ é o espaço vetorial $\mathbb{F}_2^3$.

Considere a aplicação que associa a cada par $(U, \mathcal{A}) \in (\mathcal{P}_q(n), GL_n(\mathbb{F}_q))$ um subespaço vetorial em $\mathcal{P}_q(n)$

$$\begin{array}{rcl} \phi : \mathcal{P}_q(n) \times GL_n(\mathbb{F}_q) & \to & \mathcal{P}_q(n) \\ (U, \mathcal{A}) & \mapsto & UA = rs(\mathcal{UA}). \end{array} \tag{3.22}$$

De posse da Definição 2.1.9, verifica-se que $\mathcal{P}_q(n)$ é um $GL_n(\mathbb{F}_q)-$conjunto, uma vez que a aplicação (3.22) satisfaz às seguintes condições:

(i) Dada $Id_n \in GL_n(\mathbb{F}_q)$ (matriz identidade) então, para todo $U \in \mathcal{P}_q(n)$, tem-se $\phi(U, Id_n) = rs(\mathcal{U}Id_n) = rs(\mathcal{U}) = U$.

(ii) O produto matricial é associativo, isto é, dadas três matrizes quaisquer $\mathcal{U}, \mathcal{A}, \mathcal{B} \in GL_n(\mathbb{F}_q)$, vale $(\mathcal{UA})\mathcal{B} = \mathcal{U}(\mathcal{AB})$. Em particular

$$\phi(U, \mathcal{AB}) = rs(\mathcal{U}(\mathcal{AB})) = rs((\mathcal{UA})\mathcal{B}) = \phi(UA, \mathcal{B}) \text{ e,} \tag{3.23}$$

logo, a aplicação (3.22) define uma ação (à direita) do grupo $GL_n(\mathbb{F}_q)$ sobre $\mathcal{P}_q(n)$.

Restringindo a ação (3.22) a uma dada grassmanniana $\mathcal{G}_q(n,k)$, temos

$$\begin{array}{rcl} \phi\,|_{\mathcal{G}_q(n,k)} \colon \mathcal{G}_q(n,k) \times GL_n(\mathbb{F}_q) & \to & \mathcal{G}_q(n,k) \\ (V, \mathcal{A}) & \mapsto & VA = rs(\mathcal{VA}). \end{array} \tag{3.24}$$

A ação (3.22) definida pelo grupo $GL_n(\mathbb{F}_q)$ gera uma relação de equivalência $\sim_{GL_n(\mathbb{F}_q)}$ em $\mathcal{P}_q(n)$, tal que

$$\mathcal{P}_q(n)/\sim_{GL_n(\mathbb{F}_q)} = \{\mathcal{G}_q(n,0), \mathcal{G}_q(n,1), ..., \mathcal{G}_q(n,n)\},$$

isto é, as grassmannianas $\mathcal{G}_q(n,k)$ podem ser vistas como órbitas (Definição 2.1.10). Em particular, uma grassmanniana $\mathcal{G}_q(n,k)$ pode ser particionada também em órbitas, e tal particionamento será importante para a proposta de decodificação dada no final deste capítulo.

Definição 3.2.22. *A órbita de um subgrupo G do grupo linear geral $GL_n(\mathbb{F}_q)$ sobre uma grassmanniana $\mathcal{G}_q(n,k)$ é dita um* código de órbita. *Se G é abeliano, então dizemos* código de órbita abeliano *e, em particular, se G é cíclico, então dizemos* código de órbita cíclico.

De agora em diante, focaremos principalmente em códigos de órbita cíclicos, ou em uniões de códigos de órbita cíclicos.

Denotaremos um código de órbita como $C_G(V) = \{Vg = rs(\mathcal{V}g) : g \in G\}$, onde $V \in \mathcal{G}_q(n,k)$ é dito o ponto inicial da órbita e G o grupo que age sobre V.

Observação 3.2.23. *Dado o código de órbita $C_G(V) \subset \mathcal{G}_q(n,k)$, o código complementar (Definição 3.2.6) $C_G(V)^\perp$ também é um código de órbita em $\mathcal{G}_q(n,n-k)$. De fato, conforme (TRAUTMANN F. MANGANIELLO, 2013, Theorem 18) observaram*

$$(Vg)^\perp = \left(V^\perp\right)\left(g^{-1}\right)^T, \tag{3.25}$$

onde o superíndice T denota a operação transposição de matrizes. Como G é um grupo, então os conjuntos $\left\{(g^{-1})^T : g^{-1} \in G\right\}$ e $\left\{g^T : g \in G\right\}$ são iguais. Logo, se denotarmos $G^T = \left\{g^T : g \in G\right\}$, então $C_G(V)^\perp = V^\perp G^T$.

Baseados no Teorema 2.1.12, podemos deduzir os seguintes resultados

Teorema 3.2.24. *(TRAUTMANN F. MANGANIELLO, 2013) Sejam $V \in \mathcal{G}_q(n,k)$, $G \leq GL_n(\mathbb{F}_q)$ e $C_G(V)$ um código de órbita.*

(i) $|C_G(V)| = |G|/\left|Stab_G(V)\right| = |G|/\left|G \cap Stab_{GL_n(\mathbb{F}_q)}(V)\right|$, *onde $Stab_G(V) \leq G$ descreve o estabilizador de V pela ação de G.*

(ii) A distância mínima $d_S(C_G(V))$ do código satisfaz

$$d_S(C_G(V)) = \min\left\{d_S(V, VA) : A \in T\left(G/Stab_G(V)\right),\ \text{onde } A \notin Stab_G(V)\right\}, \tag{3.26}$$

onde $T\left(G/Stab_G(V)\right)$ representa uma transversal do conjunto das classes laterais $G/Stab_G(V)$, isto é, o subconjunto minimal dos representantes das classes laterais de $G/Stab_G(V)$.

(iii) O estabilizador em $GL_n(\mathbb{F}_q)$ de diferentes palavras código $V, W \in C_G(V)$ são subgrupos conjugados, isto é, existe $\mathcal{A} \in G$ tal que

$$Stab_{GL_n(\mathbb{F}_q)}(V) = \mathcal{A}^{-1} Stab_{GL_n(\mathbb{F}_q)}(W)\mathcal{A} \text{ e } Stab_G(V) = \mathcal{A}^{-1} Stab_G(W)\mathcal{A}.$$

Além disso, $\left|Stab_{GL_n(\mathbb{F}_q)}(V)\right| = \left|Stab_{GL_n(\mathbb{F}_q)}(W)\right|$ e $|Stab_G(V)| = |Stab_G(W)|$, respectivamente.

Lema 3.2.25. *(DARAFSHEH, 2005) Se $\mathcal{A} \in GL_n(\mathbb{F}_q)$, então $ord(\mathcal{A}) \leq q^n - 1$.*

Definição 3.2.26. *Dado $\mathcal{A} \in GL_n(\mathbb{F}_q)$ tal que $ord(\mathcal{A}) = q^n - 1$, então o subgrupo $\langle\mathcal{A}\rangle < GL_n(\mathbb{F}_q)$ é dito um subgrupo de Singer e $\mathcal{A}$ um ciclo de Singer.*

De posse do Lema 3.2.25 e do Teorema 3.2.24, dado $\mathcal{A} \in GL_n(\mathbb{F}_q)$, é possível deduzir um limitante superior para a cardinalidade do código de órbita cíclico $C_{\langle\mathcal{A}\rangle}(V)$. Como $Stab_{\langle\mathcal{A}\rangle}(V)$ é um subgrupo de $\langle\mathcal{A}\rangle$ e $\mathbb{F}_q \subset Stab_{\langle\mathcal{A}\rangle}(V)$, uma vez que V é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q^n$, então

$$\left|C_{\langle\mathcal{A}\rangle}(V)\right| \leq \frac{q^n - 1}{q - 1}, \tag{3.27}$$

onde a cardinalidade máxima é atingida para o caso em que $\mathcal{A}$ é um ciclo de Singer e o estabilizador é trivial, ou seja, $Stab_{\langle\mathcal{A}\rangle}(V) = \mathbb{F}_q$.

Definição 3.2.27. *Uma matriz $\mathcal{A} \in GL_n(\mathbb{F}_q)$ é dita irredutível se $\mathbb{F}_q^n$ não contém subespaços vetoriais não triviais $\mathcal{A}-$invariantes. Do contrário, $\mathcal{A}$ é dita ser redutível. Um subespaço $V = rs(\mathcal{V}) \subset \mathbb{F}_q^n$ é dito $\mathcal{A}-$invariante se $rs(\mathcal{V}\mathcal{A}) = V$. Estendendo esta definição, dado $G \leq GL_n(\mathbb{F}_q)$, dizemos que G é irredutível se $\mathbb{F}_q^n$ não contém subespaços não triviais $G-$invariantes. Novamente, do contrário, G é dito redutível.*

Sempre que dissermos códigos de órbita cíclicos, buscaremos considerar apenas o caso em que o grupo cíclico que age sobre um dado espaço vetorial é irredutível. Tal condição é necessária para o paralelo que será traçado com os códigos de órbita descritos em (G.-LUERSSEN K. MORRISON, 2015), além de evitar redundâncias na descrição do código. A seguir, caracterizaremos as condições para que um grupo cíclico de $GL_n(\mathbb{F}_q)$ seja irredutível.

Definição 3.2.28. *A matriz companheira de um polinômio mônico $f(x) = f_0 + f_1x + ... + f_{n-1}x^{n-1} + x^n$ de grau positivo n sobre um corpo é definida como a matriz quadrada de ordem n dada por*

$$M_f = \begin{pmatrix} 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & ... & 1 \\ -f_0 & -f_1 & -f_2 & ... & -f_{n-1} \end{pmatrix}. \tag{3.28}$$

Dadas duas matrizes $\mathcal{A}, \mathcal{B} \in M_{n\times n}(\mathbb{F}_q)$, dizemos que elas são similares (ou semelhantes), se existe $\mathcal{M} \in GL_n(\mathbb{F}_q)$, tal que $\mathcal{B} = \mathcal{M}\mathcal{A}\mathcal{M}^{-1}$. Em (TRAUTMANN F. MANGANIELLO, 2013), os autores demonstram que códigos de órbita cíclicos gerados por matrizes similares dão origem a códigos isométricos, ou seja, códigos que possuem as mesmas distribuições de distância de subespaço e cardinalidade e, do ponto de vista da teoria da informação, podem ser vistos como códigos equivalentes.

Dada uma matriz $\mathcal{A} \in GL_n(\mathbb{F}_q)$, sua correspondente forma canônica racional (LANG, 2004) pode ser descrita como $FCR(\mathcal{A}) = \mathcal{S}\mathcal{A}\mathcal{S}^{-1}$, para algum $\mathcal{S} \in GL_n(\mathbb{F}_q)$.

Assim, os códigos de órbita gerados por $\langle \mathcal{A} \rangle$ e $\langle FCR(\mathcal{A}) \rangle$ são isométricos. Tem-se que $\mathcal{A}$ é irredutível se, e somente se, o polinômio característico correspondente é irredutível, e verifica-se que $FCR(\mathcal{A})$ é a matriz companheira desse polinômio.

Uma descrição completa sobre a classificação das classes de conjugação de subgrupos cíclicos de $GL_n(\mathbb{F}_q)$ e as suas aplicações para códigos de órbita pode ser vista em (MANGANIELLO; ROSENTHAL, 2011).

Portanto, de agora em diante trabalharemos apenas com matrizes companheiras de polinômios irredutíveis de grau n como geradoras dos grupos cíclicos que agem sobre um dado espaço vetorial.

Lema 3.2.29. *(TRAUTMANN F. MANGANIELLO, 2013) Sejam $p(x)$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau n e M_p sua matriz companheira. Além disso, sejam $\alpha \in \mathbb{F}_{q^n}^*$ uma raiz de $p(x)$ e φ o homomorfismo canônico*

$$\begin{array}{rcl} \varphi : \mathbb{F}_q^n & \to & \mathbb{F}_q[x]/\langle p(x) \rangle \\ (v_0, v_1, ..., v_{n-1}) & \mapsto & \displaystyle\sum_{i=0}^{n-1} v_i \alpha^i. \end{array} \tag{3.29}$$

Então, a multiplicação com M_p, respectivamente com α, comuta com a aplicação φ, isto é, para todo $v \in \mathbb{F}_q^n$, obtemos

$$\varphi(vM_p) = \varphi(v)\alpha. \tag{3.30}$$

A aplicação φ definida em (3.29) na verdade é um isomorfismo de espaços vetoriais.

Se $p(x)$ é um polinômio primitivo, então α é um elemento primitivo de $\mathbb{F}_{q^n}$ e, portanto, tem ordem $q^n - 1$. Consequentemente, a matriz M_p também terá ordem $q^n - 1$ em $GL_n(\mathbb{F}_q)$, ou seja, M_p é um ciclo de Singer, conforme visto na Definição 3.2.26.

Definição 3.2.30. *(TRAUTMANN F. MANGANIELLO, 2013) Um multiconjunto é uma generalização da noção de conjunto, onde os elementos são permitidos aparecer mais de uma vez. Para distingui-los dos conjuntos usuais $\{x \in X\}$, denotaremos um multiconjunto por $\{\{x \in X\}\}$. O número de vezes que um elemento x pertence ao multiconjunto X é dito a multiplicidade de x e será denotado por $m_X(x)$.*

Para o resultado a seguir, sejam $p(x) \in \mathbb{F}_q[x]$ um polinômio irredutível de grau n, $\alpha \in \mathbb{F}_{q^n}$ uma raiz de $p(x)$ e M_p a matriz companheira de $p(x)$. O próximo Teorema descreve uma maneira de calcular a cardinalidade e a distância mínima de um código de órbita cíclico, utilizando o conceito de multiconjunto e a identificação dada no Lema 3.2.29.

Teorema 3.2.31. *(TRAUTMANN F. MANGANIELLO, 2013) Sejam $V \in \mathcal{G}_q(n,k)$ e $G = \langle M_p \rangle \leq GL_n(\mathbb{F}_q)$. Denote por $\mathcal{O}_1, ..., \mathcal{O}_l$ as distintas órbitas de G sobre $\mathbb{F}_q^n \setminus \{0\}$.*

Assuma que tais órbitas sejam do tipo

$$\mathcal{O}_i := \left\{ p_i(\alpha)\alpha^j : j = 1, ..., ord\left(M_p\right) \right\}, \text{ para todo } i = 1, ..., l, \tag{3.31}$$

para algum $p_i(\alpha) \in \mathbb{F}_q[\alpha]$. *Então, para uma dada órbita* $\mathcal{O}_i$ *vale que, para qualquer* $u_j \in V$, *existe* $b_{(i,j)} \in \mathbb{Z}_{ord(M_p)}$ *tal que*

$$\phi\left(u_j\right) = p_i(\alpha)\alpha^{b_{(i,j)}}. \tag{3.32}$$

Para todo $i = 1, ..., l$, *defina*

$$a_{(i,\mu,\lambda)} := b_{(i,\mu)} - b_{(i,\lambda)} \tag{3.33}$$

e os multiconjuntos diferença

$$D_i := \left\{ \left\{ a_{(i,\mu,\lambda)} : \mu, \lambda \in \{1, ..., ord(P) - 1\}, \mu \neq \lambda \right\} \right\} \text{ e } D := \bigcup_{i=1}^{l} D_i. \tag{3.34}$$

Seja $\delta := \log_q\left(\max\left\{m_D(a) : a \in D\right\} + 1\right)$. *Se* $\delta < k$, *então a órbita de* G *sobre* V *é um código de cardinalidade* $ord\left(M_p\right)$ *e distância mínima* $2k - 2\delta$.

Proposição 3.2.32. *(TRAUTMANN F. MANGANIELLO, 2013) Na configuração do Teorema 3.2.31, se* $\delta = k$, *têm-se elementos da órbita com interseção completa, que corresponde ao mesmo espaço vetorial. Logo, sejam*

(i) $D' := D \setminus \left\{ \left\{ a \in D : m_D(a) = q^k - 1 \right\} \right\}$ *e* $\delta' := \log_q\left(\max\left\{m_{D'}(a) : a \in D'\right\} + 1\right)$. *Então, a distância mínima do código é* $2k - 2\delta'$.

(ii) Seja m *o menor elemento de* D *de multiplicidade* $q^k - 1$. *Então a cardinalidade do código é* m.

As demonstrações do Teorema 3.2.31 e da Proposição 3.2.32 podem ser conferidas em (ROSENTHAL, 2013).

Com base na identificação dada pelo Lema 3.2.29, agora iremos expor uma nova representação para códigos de órbita cíclicos. Os resultados e definições a seguir foram extraídos de (G.-LUERSSEN K. MORRISON, 2015), e serão utilizados constantemente neste trabalho.

Sejam $\beta \in \mathbb{F}_{q^n}$, $f(x) \in \mathbb{F}_q[x]$ o polinômio minimal de β e $M_f \in GL_n\left(\mathbb{F}_q\right)$ a respectiva matriz companheira de f. De acordo com o isomorfismo $\mathbb{F}_{q^n} \simeq \mathbb{F}_q^n$ que foi definido no Lema 3.2.29, a ação da matriz M_f sobre $\mathcal{P}_q(n)$ (ou $\mathcal{G}_q(n,k)$), vistos como conjuntos de subespaços vetoriais de $\mathbb{F}_q^n$, equivale a ação de β sobre os mesmos $\mathcal{P}_q(n)$ (ou $\mathcal{G}_q(n,k)$), porém agora vistos como conjuntos de subespaços vetoriais de $\mathbb{F}_{q^n}$.

Observação 3.2.33. *Transitaremos livremente entre estas duas representações possíveis de um dado espaço vetorial V de dimensão k, isto é, V poderá ser visto como um subespaço vetorial de $\mathbb{F}_q^n$ ou de $\mathbb{F}_{q^n}$.*

Definição 3.2.34. *Fixe um elemento β de $\mathbb{F}_{q^n}^* \setminus \{1\}$. Seja V um subespaço do $\mathbb{F}_q$-espaço vetorial $\mathbb{F}_{q^n}$. O $\beta-$código de órbita cíclico gerado por V é definido como o conjunto*

$$C_{\langle\beta\rangle}(V) := \left\{V\beta^i : i = 1, 2, ..., |\beta|\right\}. \tag{3.35}$$

Se β é primitivo em $\mathbb{F}_{q^n}$, então dizemos simplesmente código de órbita cíclico.

Buscaremos códigos de órbita cíclicos que possuam a maior cardinalidade possível e, de acordo com a Observação 3.27, uma das condições é que as órbitas devem ser geradas a partir da ação de um elemento primitivo de $\mathbb{F}_{q^n}$. Logo, de agora em diante, $\alpha \in \mathbb{F}_{q^n}$ sempre denotará um elemento primitivo de $\mathbb{F}_{q^n}$.

Dado um código de órbita cíclico $C_{\langle\alpha\rangle}(V) \subset \mathcal{G}_q(n,k)$, sem perda de generalidade, assumiremos que $1 \in V$, onde 1 denota a identidade multiplicativa do corpo $\mathbb{F}_{q^n}$. De fato, se $1 \notin V$ e $v \in V$, então os códigos $C_{\langle\alpha\rangle}(Vv^{-1})$ e $C_{\langle\alpha\rangle}(V)$ são iguais, devido ao fato de α ser primitivo em $\mathbb{F}_{q^n}$.

Definição 3.2.35. *Seja V um subespaço vetorial de $\mathbb{F}_{q^n}$. Um subcorpo $\mathbb{F}_{q^r}$ de $\mathbb{F}_{q^n}$ é chamado um amigo de V, se V é um subespaço vetorial sobre $\mathbb{F}_{q^r}$, com a multiplicação por escalar sendo a multiplicação no corpo $\mathbb{F}_{q^n}$. O maior amigo de V (com respeito à cardinalidade) é chamado o melhor amigo de V.*

Segue como uma consequência direta da Definição 3.2.35 e do Teorema 3.2.24

Proposição 3.2.36. *(G.-LUERSSEN K. MORRISON, 2015) Seja $\mathbb{F}_{q^r}$ o melhor amigo do subespaço k-dimensional V. Então*

$$\left|C_{\langle\alpha\rangle}(V)\right| = \frac{q^n-1}{q^r-1} \ e \ \left|Stab_{\langle\alpha\rangle}(V)\right| = q^r - 1. \tag{3.36}$$

Corolário 3.2.37. *(G.-LUERSSEN K. MORRISON, 2015) Seja V um subespaço k-dimensional de $\mathbb{F}_{q^n}$. Então*

$$\left|C_{\langle\alpha\rangle}(V)\right| = \frac{q^n-1}{q^k-1} \Leftrightarrow V = \mathbb{F}_{q^k}. \tag{3.37}$$

Mais ainda, $d_S\left(C_{\langle\alpha\rangle}(V)\right) = 2k$.

Definição 3.2.38. *Um código de subespaço C é dito um spread parcial se, para quaisquer palavras código $U, V \in C$, tem-se $U \cap V = \{0\}$. Se, além disso, a união de todas as palavras código cobre $\mathbb{F}_{q^n}$, ou seja,*

$$\bigcup_{V \in C} V = \mathbb{F}_{q^n}, \tag{3.38}$$

então C é dito um spread *de $\mathbb{F}_{q^n}$.*

O código de órbita cíclico descrito no Corolário 3.2.37 é um exemplo de código spread. Dentre os códigos de dimensão constante, os códigos spread atingem a maior distância mínima possível, pela própria definição destes códigos. Entretanto, tais códigos possuem uma cardinalidade reduzida se comparados, por exemplo, aos códigos de órbita cíclicos com estabilizador trivial, cuja cardinalidade é $\dfrac{q^n-1}{q-1}$.

Exemplo 3.2.39. *Seja α um elemento primitivo em $\mathbb{F}_{2^6}$. Como $\dfrac{2^6-1}{2^3-1}=9$ e $\dfrac{2^6-1}{2^2-1}=21$, então os conjuntos*

$$\left\{\alpha^{9i} : i=0,...,6\right\}\cup\{0\} \text{ e } \left\{\alpha^{21i} : i=0,1,2\right\}\cup\{0\}$$

representam os corpos $\mathbb{F}_{2^3}$ e $\mathbb{F}_{2^2}$, respectivamente. Logo, os códigos de órbita cíclicos

$$C_{\langle\alpha\rangle}\left(\mathbb{F}_{2^3}\right)=\left\{\alpha^i\mathbb{F}_{2^3} : i=0,...,8\right\} \text{ e } C_{\langle\alpha\rangle}\left(\mathbb{F}_{2^2}\right)=\left\{\alpha^i\mathbb{F}_{2^2} : i=0,...,20\right\}$$

são (6,9,6,3) e (6,21,4,2)-exemplos de códigos spread em $\mathbb{F}_{2^6}$, respectivamente.

A presença de um melhor amigo $\mathbb{F}_{q^r}$ em um subespaço vetorial V de $\mathbb{F}_{q^n}$ interfere diretamente na cardinalidade e na distância mínima do código de órbita cíclico $C_{\langle\alpha\rangle}(V)$.

A descrição do Lema 3.2.40 a seguir foi levemente alterada.

Lema 3.2.40. *(G.-LUERSSEN K. MORRISON, 2015) Sejam V um subespaço vetorial k-dimensional de $\mathbb{F}_{q^n}$ com melhor amigo $\mathbb{F}_{q^r}$, onde $\left|C_{\langle\alpha\rangle}(V)\right|=\dfrac{q^n-1}{q^r-1}$. Defina $s:=\max\limits_{1\leq j<N} dim_{\mathbb{F}_{q^r}}\left(V\cap V\alpha^j\right)$. Então*

$$d_S\left(C_{\langle\alpha\rangle}(V)\right)=2r(t-s), \text{ onde } t:=\frac{k}{r}. \tag{3.39}$$

Consequentemente,

$$2r\leq d_S\left(C_{\langle\alpha\rangle}(V)\right)\leq 2k. \tag{3.40}$$

Assim, de acordo com a Proposição 3.2.36 e o Lema 3.2.40, quanto maior for a cardinalidade do melhor amigo de V, menor será a cardinalidade do código, e maior será o limitante inferior para a distância mínima de $C_{\langle\alpha\rangle}(V)$.

A recíproca do Lema 3.2.40 não é verdadeira. De fato

Exemplo 3.2.41. *(ETZION, 2011) Sejam α um raiz do polinômio primitivo $f(x)=x^6+x+1\in\mathbb{F}_2[x]$ e $V=\{0,\alpha^0,\alpha,\alpha^4,\alpha^6,\alpha^{16},\alpha^{24},\alpha^{33}\}$ um subespaço 3-dimensional de $\mathbb{F}_{2^6}\simeq\mathbb{F}_2[x]/\langle f(x)\rangle$. Logo $C_{\langle\alpha\rangle}(V)$ é um $(6,63,4,3)-$código de subespaço, onde V tem melhor amigo trivial, neste caso, $\mathbb{F}_2$.*

A Proposição 3.2.42 a seguir e o Teorema 3.2.36 fornecem uma forma de construir códigos de órbita cíclicos com distância mínima e cardinalidade fixadas.

Proposição 3.2.42. *(G.-LUERSSEN K. MORRISON, 2015) Suponha que V é da forma $\bigoplus_{i=0}^{t-1}\alpha^{li}\mathbb{F}_{q^r}$, para algum $1 \leq l < \dfrac{q^n-1}{q^r-1}$, onde $\mathbb{F}_{q^r}$ é o melhor amigo de V. Então $d_S\left(C_{\langle\alpha\rangle}(V)\right) = 2r$.*

Conforme foi observado em (G.-LUERSSEN K. MORRISON, 2015), se na Proposição 3.2.42 não houvesse a hipótese de que $\mathbb{F}_{q^r}$ é o melhor amigo de V, poderíamos afirmar somente que $\mathbb{F}_{q^r}$ é um amigo de V.

Proposição 3.2.43. *(G.-LUERSSEN K. MORRISON, 2015) Seja $V = \bigoplus_{i=0}^{t-1}\alpha^{li}\mathbb{F}_{q^r}$, para algum $l > 1$. Denote por $f(x) \in \mathbb{F}_{q^r}[x]$ o polinômio minimal de α^l sobre $\mathbb{F}_{q^r}$. Então o $\partial(f(x)) \geq t$, onde $\partial(f(x))$ descreve o grau do polinômio $f(x)$, e*

$$V = \mathbb{F}_{q^{rt}} \Leftrightarrow \partial(f(x)) = t \Leftrightarrow \alpha^l V = V \Leftrightarrow \mathbb{F}_{q^r} \text{ não é o melhor amigo de } V.$$

Em outras palavras, $\mathbb{F}_{q^r}$ é o melhor amigo de V se, e somente se, V não é um corpo.

Proposição 3.2.44. *(G.-LUERSSEN K. MORRISON, 2015) Suponha que exista um subespaço U de V com melhor amigo $\mathbb{F}_{q^t}$, para algum $t > r$. Então $d_S\left(C_{\langle\alpha\rangle}(V)\right) \leq 2(k-t) < 2(k-r)$.*

Para quaisquer n, k e q, com $k \leq \left\lfloor \dfrac{n}{2} \right\rfloor$, não existem construções gerais para códigos de órbita cíclicos não spread $C_{\langle\alpha\rangle}(V)$ ótimos, isto é,

$$\left|C_{\langle\alpha\rangle}(V)\right| = \frac{q^n-1}{q-1} \text{ e } d_S\left(C_{\langle\alpha\rangle}(V)\right) = 2(k-1). \tag{3.41}$$

Em (TRAUTMANN F. MANGANIELLO, 2013) foi verificado que, para os parâmetros $n \in \{4, ..., 100\}$, $k \in \{1, ..., 10\}$ e $q \in \{2, 3\}$, é possível construir um código de órbita cíclico com as características apresentadas em (3.41). De posse disto, foi conjecturado que para quaisquer parâmetros n, k e q, é possível construir códigos de órbita cíclicos ótimos. Para o caso em que $k = \left\lfloor \dfrac{n}{2} \right\rfloor$, a partir de métodos computacionais, (GARCíA, 2015) afirma que não existe um código de órbita cíclico em $\mathcal{G}_2(10, 5)$ com cardinalidade $2^{10} - 1 = \dfrac{q^n-1}{q-1}$ e $d = 8 = 2(k-1)$. Em (G.-LUERSSEN K. MORRISON, 2015, Example 4.9), também foi verificado que não existe um código de órbita cíclico com $n = 8$, $k = 4$ e $q = 2$, tal que a cardinalidade do código seja 255 e a distância mínima 6. Portanto, para códigos do tipo $\left(2k, \dfrac{q^{2k}-1}{q-1}, 2(k-1), k\right)$ a conjectura não é verdadeira.

A conjectura permanece sem resposta para o caso $k < \left\lfloor \dfrac{n}{2} \right\rfloor$.

Exemplo 3.2.45. *(G.-LUERSSEN K. MORRISON, 2015) Para $q = 2$ e $n \in \{6, ..., 20\}$, o código de órbita cíclico $C_{\langle\alpha\rangle}(V)$, onde*

$$V = \mathbb{F}_2 + \alpha^2\mathbb{F}_2 + \alpha^3\mathbb{F}_2 \subset \mathbb{F}_{2^n} \tag{3.42}$$

é um subespaço 3-dimensional, possui cardinalidade $\dfrac{q^n-1}{q-1}$ e distância mínima $d = 4 = 2(k-1)$. Para $q \in \{3, 5, 7\}$ e $n \in \{6, 7, 8\}$, a mesma cardinalidade e distância mínima são obtidas.

Códigos de órbita cíclicos apresentam estruturas geométrica e algébrica bem definidas, porém a cardinalidade destes códigos, quando comparada com a cardinalidade da grassmanniana em que estão inseridos, é muito pequena. De fato

$$\left|C_{\langle\alpha\rangle}(V)\right| \leq \frac{q^n-1}{q-1} << \prod_{i=0}^{k-1} \frac{q^n-q^i}{q^k-q^i} = \left|\mathcal{G}_q(n,k)\right|. \tag{3.43}$$

Em (ETZION, 2011), é definida uma nova classe de códigos de subespaço que admite os códigos de órbita cíclicos como um caso particular.

Definição 3.2.46. *(ETZION, 2011) Um código de subespaço C é dito* cíclico *se, dado o subespaço vetorial $V \in C$ de $\mathbb{F}_{q^n}$, então $\beta V \in C$, para todo $\beta \in \mathbb{F}_{q^n}^*$.*

De agora em diante, dada a palavra código $V \in C$, diremos que $\beta V \in C$ é um deslocamento cíclico de V, para qualquer $\beta \in \mathbb{F}_{q^n}^*$.

Os códigos cíclicos não necessariamente precisam ser códigos de dimensão constante. Além disso, a partir da Definição 3.2.46, podemos observar que todo código cíclico C pode ser escrito como uma união de códigos de órbita cíclicos, isto é,

$$C = \bigcup_{i=1}^{m} C_{\langle\alpha\rangle}(V_i), \tag{3.44}$$

para subespaços vetoriais $V_i \in \mathcal{P}_q(n)$.

Exemplo 3.2.47. *(ETZION, 2011) Seja α uma raiz do polinômio primitivo $p(x) = x^8 + x^7 + x^2 + x + 1 \in \mathbb{F}_2[x]$, onde $\mathbb{F}_{2^8} \simeq \mathbb{F}_2[x]/\langle p(x)\rangle$. Considere $C \subset \mathcal{G}_2(8,3)$, que consiste de todos os deslocamentos cíclicos das palavras código*

$$\begin{aligned}
V_1 &= \left\{0, \alpha^0, \alpha^1, \alpha^{18}, \alpha^{33}, \alpha^{69}, \alpha^{99}, \alpha^{109}\right\},\\
V_2 &= \left\{0, \alpha^0, \alpha^2, \alpha^{58}, \alpha^{135}, \alpha^{163}, \alpha^{198}, \alpha^{246}\right\},\\
V_3 &= \left\{0, \alpha^0, \alpha^3, \alpha^{22}, \alpha^{82}, \alpha^{134}, \alpha^{205}, \alpha^{250}\right\},\\
V_4 &= \left\{0, \alpha^0, \alpha^4, \alpha^{24}, \alpha^{97}, \alpha^{104}, \alpha^{110}, \alpha^{141}\right\} \text{ e}\\
V_5 &= \left\{0, \alpha^0, \alpha^{12}, \alpha^{41}, \alpha^{55}, \alpha^{102}, \alpha^{125}, \alpha^{221}\right\}.
\end{aligned}$$

É verificado que $C = \bigcup_{i=1}^{5} C_{\langle\alpha\rangle}(V_i)$ é um $(8, 1275, 4, 3)-$código de subespaço cíclico ótimo.

Todo código de órbita cíclico é um código cíclico. Porém, em geral, não podemos afirmar que códigos cíclicos possam ser vistos como códigos de órbita. Em (BARDESTANI, 2015), os autores apresentam uma forma de construir códigos cíclicos, que também podem ser vistos como códigos de órbita.

Seja $N(G)$ o normalizador de um subgrupo $G \leq GL_n(\mathbb{F}_q)$, isto é,

$$N(G) := \{\mathcal{A} \in GL_n(\mathbb{F}_q) : \mathcal{A}G = G\mathcal{A}\}. \tag{3.45}$$

Dada qualquer matriz $\mathcal{A} \in N(G)$, é de verificação direta que $H = \langle G, \mathcal{A}\rangle = G \cdot \langle \mathcal{A}\rangle < GL_n(\mathbb{F}_q)$. Assim, a ação do subgrupo H sobre um subespaço vetorial k-dimensional $V = rs(\mathcal{V})$ de $\mathbb{F}_q^n$ dá origem ao seguinte código de órbita

$$C_H(V) = \bigcup_{i=0}^{ord(A)-1} C_{\langle G\rangle}\left(rs\left(\mathcal{V}\mathcal{A}^i\right)\right). \tag{3.46}$$

Sejam α um elemento primitivo de $\mathbb{F}_{q^n}$ e $\langle\sigma\rangle$ o grupo cíclico dos automorfismos de $\mathbb{F}_{q^n}$ que fixam $\mathbb{F}_q$, onde $\sigma(x) = x^q$, para todo $x \in \mathbb{F}_{q^n}$ (Teorema 2.1.45). Em particular, o normalizador $N(\langle\alpha\rangle)$ do grupo cíclico $\langle\alpha\rangle$ possui uma expressão bem simples, e ele será utilizado em vários momentos deste trabalho.

Teorema 3.2.48. *(HUPPERT, 1967) $N(\langle\alpha\rangle)$ tem ordem $n(q^n-1)$ e é isomorfo ao produto semi-direto $\langle\alpha\rangle \rtimes \langle\sigma\rangle$.*

Dado $V = \left\{0, \alpha^{i_1}, \alpha^{i_2}, ..., \alpha^{i_{q^k-1}}\right\}$ um subespaço vetorial $k-$dimensional de $\mathbb{F}_{q^n}$, a ação de $N(\langle\alpha\rangle)$ sobre V ocorre da seguinte forma

$$C_{N(\langle\alpha\rangle)}(V) = C_{\langle\alpha\rangle\rtimes\langle\sigma\rangle}(V) = \bigcup_{j=0}^{n-1} C_{\langle\alpha\rangle}\left(\sigma^j(V)\right), \tag{3.47}$$

com $\sigma^j(V) = \left\{0, \alpha^{q^j\cdot i_1}, \alpha^{q^j\cdot i_2}, ..., \alpha^{q^j\cdot i_{q^k-1}}\right\}$ também é um subespaço vetorial k-dimensional de $\mathbb{F}_{q^n}$.

Teorema 3.2.49. *(DYE, 1989) Seja n um primo ímpar. Então o normalizador de um subgrupo de Singer é um subgrupo maximal em $GL_n(\mathbb{F}_q)$.*

Exemplo 3.2.50. *Sejam $C_{N(\langle\alpha\rangle)}(V) \subset \mathcal{G}_2(5,2)$ um código de órbita, com $V = \{0, 1, \alpha, \alpha^{18}\}$ é um subespaço bidimensional de $\mathbb{F}_{2^5}$, e α uma raiz do polinômio primitivo $f(x) = x^5 + x^2 + 1 \in \mathbb{F}_2[x]$, tal que $\mathbb{F}_{2^5} \simeq \mathbb{F}_2[x]/\langle f(x)\rangle$. Logo*

$$C_{N(\langle\alpha\rangle)}(V) = \bigcup_{i=0}^{4} C_{\langle\alpha\rangle}\left(\sigma^i(V)\right), \text{ onde} \tag{3.48}$$

$$\begin{aligned}
\sigma(V) &= \left\{0, 1, \alpha^2, \alpha^5\right\}, \\
\sigma^2(V) &= \left\{0, 1, \alpha^4, \alpha^{10}\right\}, \\
\sigma^3(V) &= \left\{0, 1, \alpha^8, \alpha^{20}\right\} \text{ e} \\
\sigma^4(V) &= \left\{0, 1, \alpha^9, \alpha^{16}\right\}.
\end{aligned}$$

Portanto, $C_{N(\langle\alpha\rangle)}(V)$ é um (5,155,2,2)-código de órbita.

Dado $n \in \mathbb{N}$, temos $\left|C_{N(\langle\alpha\rangle)}(V)\right| \leq n\left(\frac{q^n-1}{q-1}\right)$, onde $\frac{q^n-1}{q-1}$ corresponde a cardinalidade do código de órbita cíclico com melhor amigo trivial (Proposição 3.2.36).

Lema 3.2.51. *(BARDESTANI, 2015) Se n é um número primo, então*

$$\left|C_{N(\langle\alpha\rangle)}(V)\right| = \left|C_{\langle\alpha\rangle}(V)\right| \text{ ou } \left|C_{N(\langle\alpha\rangle)}(V)\right| = n\left(\frac{q^n-1}{q-1}\right). \tag{3.49}$$

Os dois resultados a seguir apresentam condições que os parâmetros de um código de órbita, gerado a partir da ação de $N(\langle\alpha\rangle)$, devem satisfazer para que possa atingir a cardinalidade máxima $n\left(\frac{q^n-1}{q-1}\right)$. O enunciado do Teorema 3.2.53 foi levemente alterado.

Teorema 3.2.52. *(BARDESTANI, 2015) Sejam 2^n-1 um primo, $n \geq 5$ e V um subespaço vetorial k-dimensional de $\mathbb{F}_{2^n}$, tal que $k \neq \log_2(n+1)$ e $\sigma(V) \neq V$. Então $\left|C_{N(\langle\alpha\rangle)}(V)\right| = n\,(2^n-1)$.*

Para o caso não binário, temos o seguinte resultado.

Teorema 3.2.53. *(BARDESTANI, 2015) Seja $\frac{q^n-1}{q-1}$ um número primo, onde $n \geq 5$ e $q \neq 2$. Então*

$$\left|C_{N(\langle\alpha\rangle)}(V)\right| = n\left(\frac{q^n-1}{q-1}\right). \tag{3.50}$$

3.3 Comentários Finais

Iniciamos este capítulo, apresentando uma visão bastante geral sobre a proposta de Köetter e Kschischang para a codificação externa desenvolvida por redes lineares aleatórias. De posse destas informações, definimos códigos de subespaço e códigos de subespaço de dimensão constante. Apresentamos algumas métricas que podem ser utilizadas para a construção destes códigos, focando os resultados exclusivamente na métrica do subespaço, além de alguns limitantes (inferiores e superiores) relativos à cardinalidade dos códigos de subespaço e alguns procedimentos de decodificação mais básicos encontrados na literatura.

Em um segundo momento, foram dadas duas definições de códigos de órbita e, em particular, de códigos de órbita cíclicos, que são códigos de dimensão constante. Como o próprio nome sugere, tais códigos são órbitas de uma dada ação de um subgrupo de $GL_n(\mathbb{F}_q)$ sobre uma grassmanniana. A forma distinta com que tais definições são apresentadas decorre de como o $\mathbb{F}_q-$espaço vetorial de dimensão n é representado, a saber, $\mathbb{F}_q^n$ ou $\mathbb{F}_{q^n}$. De acordo com os problemas propostos neste trabalho, focamos na representação de $\mathcal{P}_q(n)$ visto como a coleção de subespaços de $\mathbb{F}_{q^n}$, uma vez que faremos uso constante

da estrutura algébrica deste corpo finito (visto como espaço vetorial) e dos automorfismos que atuam sobre ele. Mais ainda, desta representação, definimos os códigos spread e apresentamos um exemplo. Alguns resultados sobre cardinalidade e distância mínima de códigos de órbita são dados para ambas representações.

Conforme será visto no próximo capítulo, os códigos de órbita desenvolvem um papel central na classificação e descrição dos códigos geometricamente uniformes em $\mathcal{G}_q(n,k)$. Na verdade, existe uma equivalência entre tais definições e poderemos explorar mais profundamente as estruturas algébrica e geométrica dos códigos de órbita, fazendo uso das características oriundas do fato de serem geometricamente uniformes.

4 Códigos de Subespaço Geometricamente Uniformes

Como mencionado anteriormente, o nosso objetivo é caracterizar os códigos geometricamente uniformes definidos em $\mathcal{G}_q(n,k)$. Assim, após a definição desta classe de códigos, é observado que tal caracterização segue direto da definição de códigos de órbita e do conceito de isometria em $\mathcal{P}_q(n)$.

Na Seção 4.1 iniciamos descrevendo o conceito de códigos casados a grupos. Conforme veremos durante toda esta seção, este conceito e os demais aqui definidos são releituras de conceitos oriundos da teoria da informação clássica, adaptados para o contexto de códigos de subespaço. É imediata a conexão entre códigos casados a grupos e códigos de órbita. Em seguida, definimos o conceito principal deste trabalho, isto é, o conceito de códigos geometricamente uniformes. Após a classificação das isometrias em $\mathcal{P}_q(n)$, novamente, é de verificação imediata que tais códigos são descritos em $\mathcal{G}_q(n,k)$ pelos códigos de órbita. Assim, deduzimos alguns resultados para códigos de órbita utilizando o fato de serem geometricamente uniformes, principalmente relacionados à partição destes códigos como uma união de subcódigos isométricos. Pela analogia com os alfabetos de grupo generalizados (BIGLIERI, 1988), é possível obter um resultado relacionado à redução do número de cálculos necessários para obtenção da distância de subespaço mínima de uma classe de códigos de órbita. Além disso, dado o fato de que códigos de órbita são geometricamente uniformes, apresentamos um algoritmo de decodificação baseado no conceito de regiões de Voronoi.

Por fim, na Seção 4.2, de posse das partições geometricamente uniformes de um código de órbita, aplicamos a estas estruturas construções multiníveis, que são novamente construções clássicas, de forma que possamos garantir uma maior proteção com os códigos assim definidos a partir do uso de códigos de bloco clássicos.

4.1 Códigos de Subespaço Geometricamente Uniformes

Nesta seção apresentamos as definições de códigos casados a grupos e códigos geometricamente uniformes. É observado que tais definições, no contexto de códigos em $\mathcal{P}_q(n)$, coincidem justamente com a definição de códigos de órbita apresentada no Capítulo 3. Para uma completa caracterização dos códigos geometricamente uniformes como códigos de órbitas, é necessário classificar o conjunto de isometrias em $\mathcal{P}_q(n)$. Assim, de posse do Teorema Fundamental da Geometria Projetiva (descrito no Capítulo 2), foi ob-

servado em (TRAUTMANN, 2013b) que as transformações semilineares são justamente as isometrias no contexto em questão, e que qualquer subgrupo G de $GL_n(\mathbb{F}_q)$, que define os códigos de órbita, é exatamente um subgrupo do grupo de transformações semilineares. Logo, a caracterização é completa. De posse dos resultados relacionados às partições geometricamente uniformes e aos alfabetos de grupos generalizados, é possível obter uma visão mais geral da estrutura dos códigos de órbita.

As principais referências deste Capítulo são (BIGLIERI, 1988; JR., 1991; LOELIGER, 1991; TRAUTMANN, 2013b).

4.1.1 Códigos Casados a Grupos

Os resultados apresentados nesta subseção foram originalmente descritos em (LOELIGER, 1991) e reescritos em (GERôNIMO, 1997) em um contexto mais geral. De agora em diante, (M, d) descreverá um espaço métrico, onde d representa a métrica definida para o conjunto M.

Definição 4.1.1. *(LOELIGER, 1991) Um código finito $C \subset M$ é casado a um grupo G se existe uma aplicação sobrejetora μ de G em C tal que, para quaisquer $g_1, g_2 \in G$,*

$$d(\mu(g_1), \mu(g_2)) = d\left(\mu\left(g_1^{-1} g_2\right), \mu(e)\right), \tag{4.1}$$

onde e denota o elemento identidade de G. Uma aplicação μ satisfazendo esta condição será denominada aplicação casada. Se, mais ainda, μ é injetora, então μ será dito um rotulamento casado.

A ideia principal da Definição 4.1.1 é introduzir alguma "linearidade"para os códigos definidos em (M, d), a partir da estrutura algébrica fornecida por G.

Lema 4.1.2. *(LOELIGER, 1991) Sejam μ uma aplicação casada de um grupo G sobre um código $C \subset (M, d)$, s_e a imagem sob μ do elemento identidade de G e H definido como $\mu^{-1}(s_e)$. Então H é um subgrupo de G, e $\mu(g_1) = \mu(g_2)$ se, e somente se, $g_1 H = g_2 H$, isto é, se, e somente se, g_1 e g_2 estão na mesma classe lateral à esquerda de H em G.*

Como uma consequência do Lema 4.1.2, se H é um subgrupo normal de G, então o código C é casado ao grupo quociente G/H. Assim, dada a aplicação casada $\mu : G \to C$, podemos usar grupos quocientes de G na busca de um rotulamento casado ao código C.

Definição 4.1.3. *(LOELIGER, 1991) Uma aplicação casada de um grupo G sobre um código C é efetiva se H (definido no Lema 4.1.2) não contém um subgrupo normal não trivial de G. Se tal aplicação casada existe, então C é efetivamente casado a G.*

Teorema 4.1.4. *(LOELIGER, 1991) Se C é um código casado a um grupo G e se f é uma isometria, então $f(C)$ também é casado a G.*

Definição 4.1.5. *Dado $\Gamma(C)$ o grupo de simetrias de um código C, dizemos que um grupo G atua em C, se existe um homomorfismo $\xi : G \to \Gamma(C)$. Nessas condições, se $c \in C$, a órbita de $c \in C$, denotada por $\mathcal{O}(c)$, é o conjunto*

$$\mathcal{O}(c) = \{\xi(g)(c) : g \in G\}. \tag{4.2}$$

Se para cada par $c_1, c_2 \in C$, existe $g \in G$, tal que $\xi(g)(c_1) = c_2$, então dizemos que G é transitivo sobre C.

Definição 4.1.6. *Dados G um grupo que atua em C e $H \leq G$ então, dada uma palavra código $c \in C$, dizemos que a órbita*

$$\mathcal{O}(c) = \{\xi(h)(c) : h \in H\} \tag{4.3}$$

é um código de órbita em (M, d).

É de verificação direta que qualquer código de órbita $C_G(V) \subset \mathcal{G}_q(n, k)$ é um código casado, no caso, de forma trivial, a G. Veremos que a recíproca deste resultado também é verdadeira.

Teorema 4.1.7. *(LOELIGER, 1991) Seja G um grupo transitivo sobre o código C em um espaço métrico (M, d), ou seja, C é a órbita de uma dada palavra código sob G. Então C está casado a G e, para qualquer $c \in C$, a aplicação $\mu_c : G \to C; f \mapsto f(c)$ é uma aplicação casada. Reciprocamente, se o código C está casado a um grupo G, então existe um homomorfismo de G em um subgrupo transitivo de $\Gamma(G)$.*

De acordo com a Definição 4.1.6 e o Teorema 4.1.7, temos os seguintes resultados.

Corolário 4.1.8. *(LOELIGER, 1991) Um código C é casado a um grupo G se, e somente se, C é um código de órbita.*

Corolário 4.1.9. *(LOELIGER, 1991) Se um código C é efetivamente casado a um grupo G, então G é isomorfo a um subgrupo transitivo de $\Gamma(C)$.*

Na versão original (LOELIGER, 1991, Corollary 1), se C é um código em $(\mathbb{R}^n, d_E)$, onde d_E descreve a distância euclidiana, então C é casado a um grupo se, e somente se, C é uma translação de um código de grupo do tipo Slepian (SLEPIAN, 1968), o qual é um código de órbita sob a ação de um subgrupo do grupo das matrizes ortogonais de ordem n.

Para o espaço métrico $(\mathcal{P}_q(n), d_S)$, dados quaisquer $G \leq GL_n(\mathbb{F}_q)$ e V um subespaço vetorial k-dimensional de $\mathbb{F}_q^n$, conforme é afirmado no Corolário 4.1.8, podemos caracterizar os códigos de órbita $C_G(V)$ como os códigos casados a grupos (no caso, o grupo é o próprio G) de dimensão constante.

4.1.2 Códigos de Órbita Geometricamente Uniformes

Códigos geometricamente uniformes foram definidos por Forney em (JR., 1991). Esta classe de códigos incluí os códigos de grupo de Slepian (SLEPIAN, 1968) e os códigos reticulados (CONWAY, 1999), e foram muito utilizados nos anos 90 devido a sua estrutura algébrica e geométrica, além de apresentar diversas propriedades desejadas em teoria da informação. A definição que será dada a seguir para códigos geometricamente uniformes não está restrita apenas a códigos definidos no contexto euclidiano, conforme Forney (JR., 1991) propôs, mas em um contexto geral.

Definição 4.1.10. *Dado $C \subset (M, d)$ um código, dizemos que C é geometricamente uniforme se, dados duas palavras código c_1 e c_2 em C, existe uma isometria u_{c_1,c_2}, tal que u_{c_1,c_2} aplica c_1 em c_2 e deixa C invariante, isto é,*

$$u_{c_1,c_2}(c_1) = c_2 \text{ e } u_{c_1,c_2}(C) = C. \tag{4.4}$$

Seja C um código geometricamente uniforme. Então existe um grupo de simetrias $\Gamma(C)$ que age transitivamente sobre C, isto é, dado qualquer $c \in C$, C pode ser definido como o código de órbita

$$C = \{u(c) : u \in \Gamma(C)\}. \tag{4.5}$$

Definição 4.1.11. *Um grupo gerador G de C é um subgrupo do grupo de simetrias $\Gamma(C)$ que é minimamente suficiente para gerar C a partir de qualquer palavra código arbitrária $c \in C$. Assim, se G é um grupo gerador de C e $c \in C$, então C é a órbita de c sob G, $C = \{u(c) : u \in G\}$, e a aplicação $m : G \to C$ definida por $m(u) = u(c)$ é 1-1.*

Exemplo 4.1.12. *(JR., 1991) Considere um quadrado $Q = \{(\pm 1, \pm 1)\} \subset \mathbb{R}^2$ como um código em $\mathbb{R}^2$. Por definição, o grupo diedral D_4 é um grupo de simetrias de Q, mas este é maior que o necessário para gerar Q, pois os subgrupos*

$$G_1 = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle \simeq \mathbb{Z}_4 \text{ e } G_2 = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \simeq \mathbb{Z}_2^2 \tag{4.6}$$

agem transitivamente sob qualquer ponto de Q. Portanto, dado qualquer $q \in Q$, temos

$$Q = \{u(q) : u \in G_1\} \text{ ou } Q = \{v(q) : v \in G_2\}, \tag{4.7}$$

isto é, os grupos G_1 e G_2 são grupos geradores do código Q.

Se C é um código geometricamente uniforme, G é um grupo gerador de C e $c \in C$, então descreveremos C como $C_G(c)$.

Observação 4.1.13. *Em (WAN, 1993), o autor observou que, para códigos definidos no espaço métrico euclidiano usual $(\mathbb{R}^n, d_E)$, onde d_E denota a métrica euclidiana, existe*

uma equivalência entre códigos casados a grupos (LOELIGER, 1991) e códigos geometricamente uniformes. Conforme veremos a seguir, esta equivalência também vale para o contexto de códigos de subespaço.

As próximas duas definições desempenham um papel importante neste trabalho.

Definição 4.1.14. *Uma região de Voronoi $R_V(c_1)$ associada a uma palavra código $c_1 \in C_G(c) \subseteq (M,d)$ é o conjunto de todos os pontos em M que estão mais próximos de c_1 do que de qualquer outra palavra código $c_2 \in C_G(c)$.*

$$R_V(c_1) = \left\{ x \in M : d(c_1, x) = \min_{c_2 \in C_G(c)} d(c_2, x) \right\}. \tag{4.8}$$

Definição 4.1.15. *O perfil de distância global $DP(c_1)$ associado com qualquer palavra código $c_1 \in C_G(c) \subseteq (M,d)$ é o conjunto de distâncias para todas as outras palavras código de $C_G(c)$.*

$$DP(c_1) = \{ d(c_1, c_2), c_2 \in C_G(c) \}. \tag{4.9}$$

Após estas duas definições, podemos enunciar um dos resultados mais importantes de (JR., 1991). Ele é conhecido como *uniformidade geométrica*.

Teorema 4.1.16. *(JR., 1991) Se $C_G(c)$ é um código geometricamente uniforme em (M,d), então*

(i) Todas as regiões de Voronoi $R_V(c_1)$ têm a mesma forma e, de fato, $R_V(c_2) = u_{c_1,c_2}[R_V(c_1)]$, onde u_{c_1,c_2} é qualquer isometria que aplica c_1 em c_2,

(ii) O perfil de distância global $DP(c)$ é o mesmo para todo $c \in C_G(c)$, e o denotamos por $DP(C_G(c))$.

Exemplo 4.1.17. *Seja α uma raiz do polinômio primitivo $f(x) = x^4+x+1 \in \mathbb{F}_2[x]$, onde $\alpha \in \mathbb{F}_{2^4} \simeq \mathbb{F}_2[x]/\langle f(x) \rangle$. Além disso, dado $V_1 = \{0, 1, \alpha, \alpha^4\}$ um subespaço $2-$dimensional de $\mathbb{F}_{2^4}$, considere o código de órbita cíclico $C_{\langle\alpha\rangle}(V_1)$, onde $\left|C_{\langle\alpha\rangle}(V_1)\right| = 15$. Vamos calcular, por exemplo, o perfil de distância global das palavras código V_1 e $\alpha^7 V_1$. Do Teorema 4.1.16, o perfil de distância global destas palavras código é o mesmo. Assim, representando as palavras código $\alpha^i V$ como α^i, para $0 \leq i \leq 14$, temos*

$$DP\left(C_{\langle\alpha\rangle}(V_1)\right) = DP(V_1) = DP\left(\alpha^7 V_1\right) = 0, 2, 2, 2, 2, 2, 2, 4, 4, 4, 4, 4, 4, 4, 4 \tag{4.10}$$

Analisando a Tabela 1, observamos que $DP(\alpha^7 V_1)$ corresponde a sete deslocamentos cíclicos de $DP(V_1)$.

$\mathrm{d}_S(.,.)$	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7
α^0	0	2	4	2	2	4	4	4
α^7	4	4	4	2	2	4	2	0

$\mathrm{d}_S(.,.)$	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
α^0	4	4	4	2	2	4	2
α^7	2	4	2	2	4	4	4

Tabela 1 – Perfil de distância global das palavras código V e $\alpha^7 V$

Como $\mathcal{G}_2(4,2) = \bigcup_{i=1}^{3} C_{\langle\alpha\rangle}(V_i)$, *onde* $V_2 = \{0, 1, \alpha^2, \alpha^8\}$ *e* $V_3 = \mathbb{F}_{2^2} = \{0, 1, \alpha^5, \alpha^{10}\}$, *então a região de Voronoi da palavra código* V_1 *é*

$$\begin{aligned} R_V(V_1) &= \Big\{\alpha V_1, \alpha^3 V_1, \alpha^4 V_1, \alpha^{11} V_1, \alpha^{12} V_1, \alpha^{14} V_1, V_2, \alpha V_2, \alpha^2 V_2, \alpha^4 V_2, \alpha^7 V_2, \alpha^8 V_2, \alpha^{11} V_2, \\ &\quad \alpha^{13} V_2, \alpha^{14} V_2, V_3, \alpha V_3, \alpha^4 V_3\Big\}. \end{aligned}$$

O elemento α^{11} *age como uma simetria sobre* $C_{\langle\alpha\rangle}(V_1)$ *e, como foi visto no Teorema 4.1.16, a região de Voronoi* $u_{V_1,\alpha^{11}V_1}[R_V(V_1)] = R_V(\alpha^{11}V_1)$ *da palavra código* $\alpha^{11}V_1$ *é composta pelas seguintes palavras código*

$$\begin{aligned} R_V\left(\alpha^{11}V_1\right) &= \Big\{\alpha^{12} V_1, \alpha^{14} V_1, V_1, \alpha^7 V_1, \alpha^8 V_1, \alpha^{10} V_1, \alpha^{11} V_2, \alpha^{12} V_2, \alpha^{13} V_2, V_2, \alpha^3 V_2, \alpha^4 V_2, \\ &\quad \alpha^7 V_2, \alpha^9 V_2, \alpha^{10} V_2, \alpha V_3, \alpha^2 V_3, V_3\Big\}. \end{aligned}$$

Conforme é afirmado no Teorema 4.1.16, observa-se que códigos geometricamente uniformes possuem suas palavras código dispostas de uma forma bem definida. Ainda, dada uma única região de Voronoi, é possível obtermos todas as demais regiões de Voronoi, onde todas possuem a mesma forma e satisfazem as mesmas propriedades. Logo, podemos dizer *a* região de Voronoi de um dado código geometricamente uniforme e, conforme será visto, estes conjuntos serão úteis para o procedimento de decodificação que será proposto na próxima subseção.

A simetria dos códigos geometricamente uniformes influencia positivamente diversas propriedades desejadas em comunicações. Por exemplo, todas as palavras código têm a mesma probabilidade de erro. Para mais informações sobre outras propriedades, recomendamos a leitura de (JR., 1991).

Para uma constatação simples e natural do fato de que os códigos de órbita definidos no Capítulo 3 são geometricamente uniformes no contexto $(\mathcal{G}_q(n,k), d_S)$, vamos definir o conceito de isometria (e simetria) neste espaço métrico, além de reescrever o Teorema 2.3.26, a partir da notação utilizada neste capítulo.

Lema 4.1.18. *(TRAUTMANN, 2013b) Se* $\lambda : \mathcal{P}_q(n) \to \mathcal{P}_q(n)$ *é uma isometria, então* $\lambda(\{0\}) \in \left\{\{0\}, \mathbb{F}_q^n\right\}$.

Lema 4.1.19. *(TRAUTMANN, 2013b) Seja λ uma isometria e $V \in \mathcal{P}_q(n)$ arbitrário. Se $\lambda(\{0\}) = \{0\}$, então*

$$dim(V) = d_S(\{0\}, V) = d_S(\{0\}, \lambda(V)) = dim\lambda(V). \tag{4.11}$$

Do contrário, $\lambda(\{0\}) = \mathbb{F}_q^n$, e

$$dim(V) = d_S(\{0\}, V) = d_S\left(\mathbb{F}_q^n, \lambda(V)\right) = n - dim\lambda(V). \tag{4.12}$$

Para preservar a dimensão das palavras código e, consequentemente, para as propostas de cálculo de distância de subespaço mínima de códigos de órbita, suporemos que todas as isometrias em questão satisfazem à condição (4.11).

Para os próximos resultados, considere $q = p^n$, onde p é um número primo. Reescrevendo o Teorema 2.3.26 temos

Teorema 4.1.20. *(TRAUTMANN, 2013b) Toda isometria λ em $\mathcal{P}_q(n)$, com $n > 2$ e $dim(V) = dim(\lambda(V))$, para qualquer $V \in \mathcal{P}_q(n)$, é induzida por uma transformação semilinear $(A, \sigma_i) \in P\Gamma L_n(\mathbb{F}_q)$, tal que $P\Gamma L_n(\mathbb{F}_q) := (GL_n(\mathbb{F}_q)/Z_n(\mathbb{F}_q)) \rtimes Aut(\mathbb{F}_q)$, onde $Aut(\mathbb{F}_q)$ descreve o grupo dos automorfismos de $\mathbb{F}_q$ que fixam o subcorpo primo $\mathbb{F}_p$.*

Teorema 4.1.21. *(TRAUTMANN, 2013b) Para qualquer $n > 2$, uma aplicação $\lambda : \mathcal{P}_q(n) \to \mathcal{P}_q(n)$ é uma bijeção que preserva a ordem (com respeito a relação de inclusão) de $\mathcal{P}_q(n)$ se, e somente se, λ é uma isometria com $\lambda(\{0\}) = \{0\}$.*

Corolário 4.1.22. *(TRAUTMANN, 2013b) Toda isometria λ em $\mathcal{P}_q(n)$, com $n > 2$ e com $dim(V) = dim(\lambda(V))$, para qualquer $V \in \mathcal{P}_q(n)$, é induzida por uma transformação semilinear $(A, \varphi) \in P\Gamma L_n(\mathbb{F}_q)$.*

Agora, estamos aptos a caracterizar os códigos de órbita como códigos geometricamente uniformes em $\mathcal{G}_q(n, k)$.

Proposição 4.1.23. *Dado $C \subseteq \mathcal{G}_q(n, k)$, C é um código de subespaço geometricamente uniforme se, e somente se, $C = C_G(V)$ é um código de órbita, onde $G \leq P\Gamma L_n(\mathbb{F}_q)$.*

Demonstração. Sejam $G \leq P\Gamma L_n(\mathbb{F}_q)$ e V um subespaço vetorial de dimensão k de $\mathbb{F}_q^n$. De acordo com a Definição 4.1.10, todo código geometricamente uniforme em $\mathcal{G}_q(n, k)$ é um código de órbita $C_G(V)$. Reciprocamente, se $C_G(V)$ é um código de órbita então, pelo Corolário 4.1.22, os elementos de G agem como isometrias em $\mathcal{P}_q(n)$ e, em particular, G age como um grupo de simetrias de $C_G(V)$, pois para quaisquer duas palavras código distintas $Vg_i, Vg_j \in C_G(V)$, para $0 \leq i \leq j \leq |G| - 1$, a estrutura de grupo garante a existência de uma simetria que aplica Vg_i em Vg_j. De fato, basta aplicar a simetria $g_i^{-1}g_j \in G$ sobre Vg_i. □

Seja α um elemento primitivo de $\mathbb{F}_{q^n}$, $n > 2$, e considere o código de dimensão constante $C = C_{\langle\alpha\rangle}(V) \cup C_{\langle\alpha\rangle}(\sigma(V))$, onde $\sigma(x) = x^q$, para qualquer $x \in \mathbb{F}_{q^n}$, denota o automorfismo de Frobenius. Este código é um código cíclico, uma vez que é fechado para o deslocamento cíclico de qualquer palavra código por α, mas não é um código de órbita.

Corolário 4.1.24. *Códigos de subespaço cíclicos são geometricamente uniformes se, e somente se, são códigos de órbita*

O Corolário 4.1.24 pode ser reescrito como: Em geral, a união de códigos geometricamente uniformes não implica em um código geometricamente uniforme. Como um exemplo de código de subespaço cíclico geometricamente uniforme, consideremos o produto semi-direto dos grupos $\langle\alpha\rangle \rtimes \langle\sigma\rangle$. Dado V um subespaço $k-$dimensional, o código $C_{\langle\alpha\rangle\rtimes\langle\sigma\rangle}(V) \subset \mathcal{G}_q(n,k)$ pode ser escrito como

$$C_{\langle\alpha\rangle\rtimes\langle\sigma\rangle}(V) = \bigcup_{i=0}^{n-1} C_{\langle\alpha\rangle}\left(\sigma^i(V)\right), \tag{4.13}$$

ou seja, este código é cíclico (na verdade é um código de órbita) e geometricamente uniforme.

Dado $C_G(c)$ um código geometricamente uniforme, seja $H \lhd G$ um subgrupo normal de G. Forney (JR., 1991) definiu uma *partição geometricamente uniforme* como uma partição de $C_G(c)$ gerada pelo grupo quociente $G/H = \{Hg_1, Hg_2, ..., Hg_t\}$, onde $t = |G/H|$ e g_1 é o elemento identidade de G. Então, dada uma classe lateral de G/H, definimos o subcódigo

$$C_{Hg_i}(c) = \{h\left(g_i(c)\right) : h \in H\}, \tag{4.14}$$

tal que $C_G(c) = \bigcup_{i=1}^{t} C_{Hg_i}(c)$, ou seja, $C_G(c)$ pode ser particionado a partir de um subgrupo normal de G. De imediato, verifica-se que não há apenas uma única forma de particionar $C_G(c)$ fazendo uso da estrutura de G.

Teorema 4.1.25. *(JR., 1991) Seja $C_{G/H}(c) = \{C_{Hg_1}(c), C_{Hg_2}(c), ..., C_{Hg_t}(c)\}$ uma partição geometricamente uniforme de $C_G(c)$. Então os subcódigos $C_{Hg_i}(c)$ de $C_G(c)$ nesta partição são geometricamente uniformes, mutualmente congruentes e possuem H como grupo gerador comum.*

Uma partição geometricamente uniforme de um código de órbita está diretamente relacionada com a estrutura do grupo gerador que dá origem ao código. A escolha de uma partição adequada, conforme veremos a seguir, resulta, por exemplo, em uma redução do número de operações necessárias para o cálculo da distância de subespaço mínima do código de órbita. Para este propósito, apresentamos alguns resultados e definições relativos aos subgrupos normais de $GL_n\left(\mathbb{F}_q\right)$, de forma a oferecer uma caracterização completa dos

códigos de órbita e as suas partições geometricamente uniformes. Estes resultados foram extraídos de (ROTMAN, 1995; SUPRUNENKO, 1976).

A notação do próximo teorema (Teorema 4.1.26) foi levemente alterada, uma vez que ele foi descrito para anéis de divisão (ver (LIDL, 1997)), que têm corpos finitos como um caso particular.

Teorema 4.1.26. *(SUPRUNENKO, 1976) Dado $n > 1$, então todo subgrupo de $GL_n(\mathbb{F}_q)$ que contém $SL_n(\mathbb{F}_q)$ (grupo linear especial) ou está contido em $Z_n(\mathbb{F}_q)$ é um subgrupo normal de $GL_n(\mathbb{F}_q)$. Se $n > 2$, ou $n = 2$ mas $q \neq 2$ ou $q \neq 3$, então qualquer subgrupo normal de $GL_n(\mathbb{F}_q)$ contém $SL_n(\mathbb{F}_q)$ ou está contido no centro de $GL_n(\mathbb{F}_q)$, que é justamente $Z_n(\mathbb{F}_q)$.*

Definição 4.1.27. *Uma série normal de um grupo G, onde e é o elemento identidade de G, é uma sequência de subgrupos*

$$G = G_0 \geq G_1 \geq ... \geq G_{m-1} \geq G_m = \{e\}, \tag{4.15}$$

onde $G_{i+1} \lhd G_i$, para todos $i = 0, ..., m-1$.

Uma série de composição é uma série normal

$$G = G_0 \geq G_1 \geq ... \geq G_{m-1} \geq G_m = \{e\}, \tag{4.16}$$

onde, para todos $i = 0, ..., m-1$, ou G_{i+1} é um subgrupo normal maximal de G_i, ou $G_{i+1} = G_i$.

O próximo exemplo (Exemplo 4.1.28) apresenta uma cadeia de subgrupos normais, os quais podem ser usados para construir sucessivas partições geometricamente uniformes.

Exemplo 4.1.28. *(ROTMAN, 1995) Se t é um inteiro não negativo e α é um elemento primitivo de $\mathbb{F}_q$, então considere o seguinte conjunto*

$$M(t) = \left\{ A \in GL_n(\mathbb{F}_q) : \ det(A) \text{ é uma potência de } \alpha^t \right\}. \tag{4.17}$$

É de verificação direta que $M(t)$ é um subgrupo de $GL_n(\mathbb{F}_q)$.

Se $|GL_n(\mathbb{F}_q)| = M$ e t é um divisor de $q-1$, então $M(t)$ é um subgrupo normal de $GL_n(\mathbb{F}_q)$, cuja ordem é M/t. Além disso, se $q - 1 = \prod_{i=1}^{r} p_i$, onde os p_i são números primos não necessariamente distintos, então a seguinte série normal

$$GL_n(\mathbb{F}_q) = M(1) > M(p_1) > M(p_1 p_2) > ... > M(q-1) > \{Id_n\} \tag{4.18}$$

é o começo de uma série de composição de $GL_n(\mathbb{F}_q)$.

Agora, apresentamos alguns conceitos de (BIGLIERI, 1988), adaptados para a linguagem deste trabalho, que são úteis para a nossa proposta de reduzir o número mínimo de cálculos necessários para obter a distância mínima de um código de órbita gerado por um grupo abeliano.

Seja $B \subseteq \mathcal{P}_q(n)$. Definimos o *conjunto intradistância* $D_S(B)$ como o multiconjunto de todas as distâncias de subespaço entre os pares de subespaços de B, isto é,

$$D_S(B) := \{\{d_S(V_1, V_2) : V_1, V_2 \in B\}\}. \tag{4.19}$$

Quando $B = C_G(V)$, para $G < GL_n(\mathbb{F}_q)$, o cálculo da distância mínima de $D_S(B)$ coincide com a distância mínima $d_S(C_G(V))$ de $C_G(V)$, a qual é computada como

$$d_S(C_G(V)) = \min\{d_S(V, VA) : A \in G \setminus \{Id_n\}\}. \tag{4.20}$$

Se B_1 e B_2 são dois conjuntos disjuntos de $\mathcal{P}_q(n)$, o *conjunto interdistância* $D_S(B_1, B_2)$ é o multiconjunto de todas as distâncias de subespaço entre subespaços de B_1 e de B_2

$$D_S(B_1, B_2) := \{\{d_S(V_1, V_2) : V_1 \in B_1 \text{ e } V_2 \in B\}\}. \tag{4.21}$$

Definição 4.1.29. *Considere uma partição $B_1, B_2, ..., B_m$ de um conjunto $X \subseteq \mathcal{G}_q(n,k)$. Tal partição é justa se, para cada $1 \leq i \neq j \leq m$,*

(i) $B_i \neq B_j$,

(ii) $|B_i| = |B_j|$ *e*

(iii) $D_S(B_i) = D_S(B_j)$.

Dado $H \lhd G$, o Teorema 4.1.25 afirma que todas as partições geometricamente uniformes $C_{G/H}(V)$ resultam em partições justas.

Definição 4.1.30. *Uma cadeia de partições de um conjunto $X \subseteq \mathcal{G}_q(n,k)$ é chamada justa se quaisquer dois conjuntos da partição, no mesmo nível da cadeia, possuem o mesmo número de elementos e têm conjuntos intradistâncias iguais.*

Novamente, dada uma série normal $G = G_0 \geq G_1 \geq ... \geq G_m \neq \{Id_n\}$ de $G < GL_n(\mathbb{F}_q)$, por sucessivas aplicações do Teorema 4.1.25, observamos que todas as partições nos diferentes níveis são justas e, portanto, temos uma cadeia de partições, em conformidade com o que é estabelecido na Definição 4.1.30. Trata-se de um caso particular de (BIGLIERI, 1988, Theorem 2).

Exemplo 4.1.31. *Sejam $p(x) = x^6 + x + 1 \in \mathbb{F}_2[x]$ um polinômio primitivo em $\mathbb{F}_2[x]$, $\alpha \in \mathbb{F}_{2^6} \simeq \mathbb{F}_2[x]/\langle p(x)\rangle$ uma raiz de $p(x)$ e $V = \{0, 1, \alpha^8, \alpha^{10}, \alpha^{20}, \alpha^{48}, \alpha^{59}, \alpha^{61}\}$ um subespaço*

3-*dimensional de* $\mathbb{F}_{2^6}$. *Dada a série de composição* $\langle\alpha\rangle > \langle\alpha^3\rangle > \langle\alpha^9\rangle$, *obtemos a seguinte cadeia de partições de* $C_{\langle\alpha\rangle}(V)$

$$\begin{aligned} C_{\langle\alpha\rangle}(V) &= \bigcup_{i=0}^{2} C_{\langle\alpha^3\rangle}\left(\alpha^i V\right) \\ &= \bigcup_{i=0}^{8} C_{\langle\alpha^9\rangle}\left(\alpha^i V\right). \end{aligned} \tag{4.22}$$

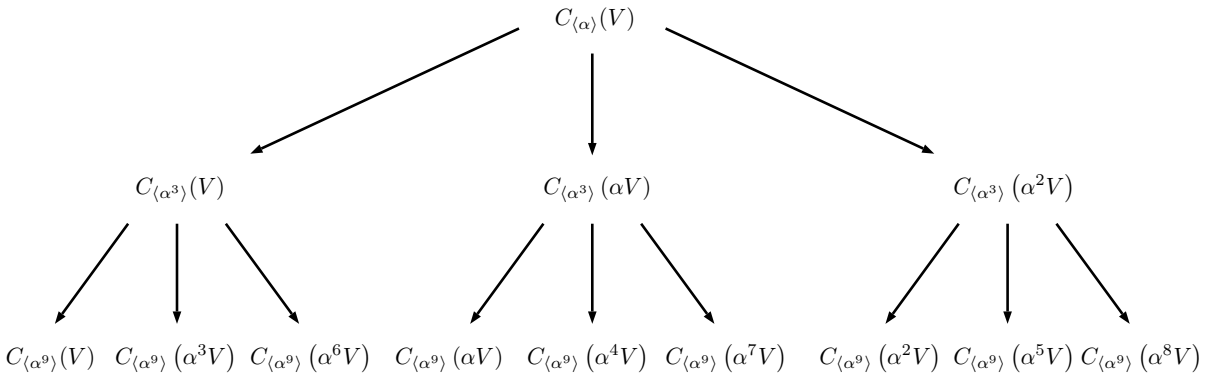


Figura 6 – Exemplo de uma cadeia de partições

Definição 4.1.32. *Dados* $H \lhd G$ *e* $g_i \in G$, *sejam* $C_H(V_i) = C_H(g_i V)$ *um subcódigo de* $C_G(V)$ *(uma classe lateral da partição geometricamente uniforme (justa)* $C_{G/H}(V)$*) e* $g_i \neq g \in G$. *O perfil de distância associado com* g *e* $C_H(V_i)$ *é representado pelo polinômio na indeterminada* w

$$F(w, g, C_H(V_i)) = \sum_d a(d) w^d, \tag{4.23}$$

onde $a(d)$ *é o número de elementos de* $C_H(V_i)$ *que distam (via a distância de subespaço)* d *com respeito a um elemento de* $C_H(gV_i) = C_H(gg_iV)$.

Exemplo 4.1.33. *Dado* $p(x) = x^6 + x + 1 \in \mathbb{F}_2[x]$ *um polinômio primitivo, sejam* α *uma raiz de* $p(x)$, *onde* $\alpha \in \mathbb{F}_{2^6} \simeq \mathbb{F}_2[x]/\langle p(x)\rangle$, *e* $V = \{0, 1, \alpha^8, \alpha^{10}, \alpha^{20}, \alpha^{48}, \alpha^{59}, \alpha^{61}\}$ *um subespaço* $3-$*dimensional de* $\mathbb{F}_{2^6}$. *O código de órbita cíclico* $C_{\langle\alpha^3\rangle}(V)$ *pode ser particionado como*

$$C_{\langle\alpha^3\rangle}(V) = \bigcup_{i=0}^{2} C_{\langle\alpha^9\rangle}\left(\alpha^i V\right), \text{ onde} \tag{4.24}$$

$$\begin{aligned} C_{\langle\alpha^9\rangle}(V) &:= \left\{\alpha^{9i} V : 0 \leq i \leq 6\right\} \\ &= \Big\{\left\{0, 1, \alpha^8, \alpha^{10}, \alpha^{20}, \alpha^{48}, \alpha^{59}, \alpha^{61}\right\}, \left\{0, \alpha^5, \alpha^7, \alpha^9, \alpha^{17}, \alpha^{19}, \alpha^{29}, \alpha^{57}\right\}, \\ &\quad \left\{0, \alpha^3, \alpha^{14}, \alpha^{16}, \alpha^{18}, \alpha^{26}, \alpha^{28}, \alpha^{38}\right\}, \left\{0, \alpha^{12}, \alpha^{23}, \alpha^{25}, \alpha^{27}, \alpha^{35}, \alpha^{37}, \alpha^{47}\right\}, \\ &\quad \left\{0, \alpha^{21}, \alpha^{32}, \alpha^{34}, \alpha^{36}, \alpha^{44}, \alpha^{46}, \alpha^{56}\right\}, \left\{0, \alpha^2, \alpha^{30}, \alpha^{41}, \alpha^{43}, \alpha^{45}, \alpha^{53}, \alpha^{55}\right\}, \\ &\quad \left\{0, \alpha, \alpha^{11}, \alpha^{39}, \alpha^{50}, \alpha^{52}, \alpha^{54}, \alpha^{62}\right\}\Big\}, \end{aligned}$$

$$
\begin{aligned}
C_{\langle\alpha^9\rangle}\left(\alpha^3V\right) &:= \left\{\alpha^{9i+3}V : 0 \leq i \leq 6\right\} \\
&= \Big\{\Big\{0,\alpha,\alpha^3,\alpha^{11},\alpha^{13},\alpha^{23},\alpha^{51},\alpha^{62}\Big\},\Big\{0,\alpha^8,\alpha^{10},\alpha^{12},\alpha^{20},\alpha^{22},\alpha^{32},\alpha^{60}\Big\}, \\
&\quad \Big\{0,\alpha^6,\alpha^{17},\alpha^{19},\alpha^{21},\alpha^{29},\alpha^{31},\alpha^{41}\Big\},\Big\{0,\alpha^{15},\alpha^{26},\alpha^{28},\alpha^{30},\alpha^{38},\alpha^{40},\alpha^{50}\Big\}, \\
&\quad \Big\{0,\alpha^{24},\alpha^{35},\alpha^{37},\alpha^{39},\alpha^{47},\alpha^{49},\alpha^{59}\Big\},\Big\{0,\alpha^5,\alpha^{33},\alpha^{44},\alpha^{46},\alpha^{48},\alpha^{56},\alpha^{58}\Big\}, \\
&\quad \Big\{0,\alpha^2,\alpha^4,\alpha^{14},\alpha^{42},\alpha^{53},\alpha^{55},\alpha^{57}\Big\}\Big\} \ \ e \\
C_{\langle\alpha^9\rangle}\left(\alpha^6V\right) &:= \left\{\alpha^{9i+6}V : 0 \leq i \leq 6\right\} \\
&= \Big\{\Big\{0,\alpha^2,\alpha^4,\alpha^6,\alpha^{14},\alpha^{16},\alpha^{26},\alpha^{54}\Big\},\Big\{0,1,\alpha^{11},\alpha^{13},\alpha^{15},\alpha^{23},\alpha^{25},\alpha^{35}\Big\}, \\
&\quad \Big\{0,\alpha^9,\alpha^{20},\alpha^{22},\alpha^{24},\alpha^{32},\alpha^{34},\alpha^{44}\Big\},\Big\{0,\alpha^{18},\alpha^{29},\alpha^{31},\alpha^{33},\alpha^{41},\alpha^{43},\alpha^{53}\Big\}, \\
&\quad \Big\{0,\alpha^{27},\alpha^{38},\alpha^{40},\alpha^{42},\alpha^{50},\alpha^{52},\alpha^{62}\Big\},\Big\{0,\alpha^8,\alpha^{36},\alpha^{47},\alpha^{49},\alpha^{51},\alpha^{59},\alpha^{61}\Big\}, \\
&\quad \Big\{0,\alpha^5,\alpha^7,\alpha^{17},\alpha^{45},\alpha^{56},\alpha^{58},\alpha^{60}\Big\}\Big\}.
\end{aligned}
$$

Os polinômios $F\left(w,\alpha^3,C_{\langle\alpha^9\rangle}(V)\right)$ *e* $F\left(w,\alpha^6,C_{\langle\alpha^9\rangle}(V)\right)$ *são obtidos a partir dos conjuntos interdistâncias* $D_S\left(C_{\langle\alpha^9\rangle}(V),C_{\langle\alpha^9\rangle}\left(\alpha^3V\right)\right)$ *e* $D_S\left(C_{\langle\alpha^9\rangle}(V),C_{\langle\alpha^9\rangle}\left(\alpha^6V\right)\right)$*, respectivamente. Logo, mais uma vez representando a palavra código* α^iV *como* α^i*, temos*

$\mathrm{d}_S(.,.)$	α^3	α^{12}	α^{21}	α^{30}	α^{39}	α^{48}	α^{57}
α^0	6	2	6	6	4	4	6
α^9	6	6	2	6	6	4	4
α^{18}	4	6	6	2	6	6	4
α^{27}	4	4	6	6	2	6	6
α^{36}	6	4	4	6	6	2	6
α^{45}	6	6	4	4	6	6	2
α^{54}	2	6	6	4	4	6	6

Tabela 2 – Conjunto interdistância $D_S\left(C_{\langle\alpha^9\rangle}(V),C_{\langle\alpha^9\rangle}\left(\alpha^3V\right)\right)$

$\mathrm{d}_S(.,.)$	α^6	α^{15}	α^{24}	α^{33}	α^{42}	α^{51}	α^{60}
α^0	6	4	4	6	6	2	6
α^9	6	6	4	4	6	6	2
α^{18}	2	6	6	4	4	6	6
α^{27}	6	2	6	6	4	4	6
α^{36}	6	6	2	6	6	4	4
α^{45}	4	6	6	2	6	6	4
α^{54}	4	4	6	6	2	6	6

Tabela 3 – Conjunto interdistância $D_S\left(C_{\langle\alpha^9\rangle}(V),C_{\langle\alpha^9\rangle}\left(\alpha^6V\right)\right)$

Portanto, de posse das Tabelas 2 *e* 3*, verificamos*

$$F\left(w,\alpha^3,C_{\langle\alpha^9\rangle}(V)\right) = F\left(w,\alpha^6,C_{\langle\alpha^9\rangle}(V)\right) = 7w^2+14w^4+28w^6. \tag{4.25}$$

O fato de que os polinômios $F\left(w, \alpha^3, C_{\langle\alpha^9\rangle}(V)\right)$ e $F\left(w, \alpha^6, C_{\langle\alpha^9\rangle}(V)\right)$ são os mesmos no Exemplo 4.1.33 não é uma coincidência.

Definição 4.1.34. *A partição geometricamente uniforme* $C_{G/H}(V) = \{C_H(g_1V), ..., C_H(g_tV)\}$ *é dita homogênea se o conjunto* $\{F(w, g_i, C_H(g_jV))\}_{g_i \in G/H}$ *não depende de* $C_H(g_jV)$. *Ela é dita fortemente homogênea se* $F(w, g_i, C_H(g_jV))$ *não depende de* $C_H(g_jV)$, *para qualquer* $g_i \in G/H$.

Teorema 4.1.35. *(BIGLIERI, 1988) Se* G *é um grupo abeliano de* $GL_n(\mathbb{F}_q)$, *todas as partições geometricamente uniformes geradas por subgrupos de* G *são fortemente homogêneas.*

Lema 4.1.36. *Dados* $G < GL_n(\mathbb{F}_q)$ *um grupo abeliano,* H *um subgrupo de* G *e* $C_G(V)$ *um código de órbita, seja* $C_{G/H}(V) = \{C_H(g_1V), C_H(g_2V), ..., C_H(g_tV)\}$ *uma partição geometricamente uniforme de* $C_G(V)$. *Então, para qualquer* $g_i \in G/H$, *temos*

$$F(w, g_i, C_H(V)) = F\left(w, g_i^{-1}, C_H(V)\right), \tag{4.26}$$

para todo $0 \leq i \leq t-1$.

Demonstração. Cada polinômio $F(w, g_i, C_H(V))$ é calculado a partir do conjunto interdistância $D_S(C_H(g_iV), C_H(V))$. Este conjunto é descrito como

$$\begin{aligned} D_S(C_H(g_iV), C_H(V)) &= \{\{d_S(h_jg_iV, h_kV)\}\} \\ &= \{\{d_S(g_ih_jV, h_kV)\}\} \\ &= \left\{\left\{d_S\left(h_jV, g_i^{-1}h_kV\right)\right\}\right\} \\ &= \left\{\left\{d_S\left(h_jV, h_kg_i^{-1}V\right)\right\}\right\} \\ &= D_S\left(C_H\left(g_i^{-1}V\right), C_H(V)\right), \end{aligned}$$

para $h_j, h_k \in H$. Como $D_S(C_H(g_iV), C_H(V)) = D_S\left(C_H\left(g_i^{-1}V\right), C_H(V)\right)$, então o resultado segue. □

O Lema 4.1.36 justifica porquê os polinômios $F\left(w, \alpha^3, C_{\langle\alpha^9\rangle}(V)\right)$ e $F\left(w, \alpha^6, C_{\langle\alpha^9\rangle}(V)\right)$ do Exemplo 4.1.33 são iguais.

Para um código de órbita $C_G(V)$, onde G é um subgrupo abeliano de $GL_n(\mathbb{F}_q)$, o próximo resultado garante que não há necessidade de calcular todas as distâncias $d_S(V, Vg_i)$, para $2 \leq i \leq |G|$, para obter a distância mínima deste código.

Teorema 4.1.37. *Dados* $G < GL_n(\mathbb{F}_q)$ *um grupo abeliano,* H *um subgrupo de* G *e* $C_G(V)$ *um código de órbita, sejam* $C_{G/H}(V) = \{C_H(g_1V), C_H(g_2V), ..., C_H(g_tV)\}$ *uma partição geometricamente uniforme de* $C_G(V)$, *onde* $C_H(g_1V) = C_H(V)$, $G/H = \left\{g_1, g_2, ..., g_{\frac{t}{2}}, g_2^{-1}, ..., g_{\frac{t}{2}}^{-1}\right\}$ *e* $I = \left\{2, ..., \frac{t}{2}\right\}$. *Então*

$$d_S(C_G(V)) = \min_{i \in I}\{D_S(\{V\}, C_H(g_iV))\}. \tag{4.27}$$

Demonstração. A distância de subespaço mínima de $C_G(V)$ é calculada como

$$d_S\left(C_G(V)\right) = \min\left\{d_S\left(V, g_iV\right) : g_i \in G \setminus \{g_1\}\right\}. \tag{4.28}$$

Pelo Teorema 4.1.25, esta distância também pode ser obtida como

$$d_S\left(C_G(V)\right) = \min\left\{d_S\left(C_H(V)\right), \min_{g_i \in G/H \setminus \{g_1\}} \left\{D_S\left(C_H(V), C_H\left(g_iV\right)\right)\right\}\right\}. \tag{4.29}$$

A distância de subespaço mínima no conjunto interdistância $D_S\left(C_H(V), C_H\left(g_iV\right)\right)$ pode ser calculada a partir da análise da distância de subespaço mínima no conjunto interdistância

$$D_S\left(\{V\}, C_H\left(g_iV\right)\right), \tag{4.30}$$

uma vez que, para qualquer $h \in H$, o perfil de distância de $D_S\left(\{hV\}, C_H\left(g_iV\right)\right)$ é simplesmente uma permutação do perfil de distância obtido em (4.30).

De acordo com o Lema 4.1.36, os polinômios $F\left(w, g_i, C_H(V)\right)$ e $F\left(w, g_i^{-1}, C_H(V)\right)$ são os mesmos e, consequentemente, os conjuntos interdistâncias $D_S\left(C_H\left(g_iV\right), C_H(V)\right)$ e $D_S\left(C_H\left(g_i^{-1}V\right), C_H(V)\right)$ também são iguais. Logo, a Equação (4.29) pode ser reescrita como

$$d_S\left(C_G(V)\right) = \min\left\{d_S\left(C_H(V)\right), \min_{i \in I}\left\{D_S\left(\{V\}, C_H\left(g_iV\right)\right)\right\}\right\}. \tag{4.31}$$

Como $d_S\left(C_H(V)\right) \geq d_S\left(C_G(V)\right)$, então $d_S\left(C_H(V)\right) \geq \min_{i \in I}\left\{D_S\left(\{V\}, C_H\left(g_iV\right)\right)\right\}$. Portanto, basta apenas calcularmos $\min_{i \in I}\left\{D_S\left(\{V\}, C_H\left(g_iV\right)\right)\right\}$ para obtermos a distância de subespaço mínima de $C_G(V)$. □

Observação 4.1.38. *Seguindo a notação do Teorema 4.1.37, dado $g \in G/H$, onde $g \neq g_1$ e $ord(g) = 2$, então consideramos que $g \in I$.*

No Exemplo 4.1.33, de acordo com o Teorema 4.1.37, em vez de realizarmos 20 cálculos para obtermos a distância de subespaço mínima de $C_{\langle\alpha^3\rangle}(V)$, basta calcularmos a distância mínima de $D_S\left(\{V\}, C_{\langle\alpha^9\rangle}\left(\alpha^3V\right)\right)$ ou $D_S\left(\{V\}, C_{\langle\alpha^9\rangle}\left(\alpha^6V\right)\right)$, totalizando apenas 7 cálculos.

Exemplo 4.1.39. *Sejam $p(x) = x^6 + x + 1 \in \mathbb{F}_2[x]$ um polinômio primitivo e $\alpha \in \mathbb{F}_{2^6} \simeq \mathbb{F}_2[x]/\langle p(x)\rangle$ uma raiz de $p(x)$. Dado $V = \{0, \alpha^0, \alpha^1, \alpha^4, \alpha^6, \alpha^{16}, \alpha^{24}, \alpha^{33}\}$ um subespaço $3-$dimensional de $\mathbb{F}_{2^6}$, vamos obter a distância de subespaço mínima do código de órbita cíclico $C_{\langle\alpha\rangle}(V)$.*

Como a $ord(\alpha) = 63$, tome $H = \langle\alpha^9\rangle$, onde $|H| = 7$. Assim, a partição geometricamente uniforme $C_{G/H}(V)$ é descrita como

$$\begin{aligned} C_{G/H}(V) \;=\; & \left\{C_H(V), C_H(\alpha V), C_H\left(\alpha^2V\right), C_H\left(\alpha^3V\right), C_H\left(\alpha^4V\right), C_H\left(\alpha^5V\right), C_H\left(\alpha^6V\right)\right. \\ & \left. C_H\left(\alpha^7V\right), C_H\left(\alpha^8V\right)\right\}, \text{ onde} \end{aligned}$$

$$
\begin{aligned}
C_H(\alpha V) &:= \left\{\alpha^{9i+1}V : 0 \leq i \leq 6\right\} \\
&= \Big\{\left\{0, \alpha^1, \alpha^2, \alpha^5, \alpha^7, \alpha^{17}, \alpha^{25}, \alpha^{34}\right\}, \left\{0, \alpha^{10}, \alpha^{11}, \alpha^{14}, \alpha^{16}, \alpha^{26}, \alpha^{34}, \alpha^{43}\right\}, \\
&\quad \left\{0, \alpha^{19}, \alpha^{20}, \alpha^{23}, \alpha^{25}, \alpha^{35}, \alpha^{43}, \alpha^{52}\right\}, \left\{0, \alpha^{28}, \alpha^{29}, \alpha^{32}, \alpha^{34}, \alpha^{44}, \alpha^{52}, \alpha^{61}\right\}, \\
&\quad \left\{0, \alpha^7, \alpha^{37}, \alpha^{38}, \alpha^{41}, \alpha^{43}, \alpha^{53}, \alpha^{61}\right\}, \left\{0, \alpha^7, \alpha^{16}, \alpha^{46}, \alpha^{47}, \alpha^{50}, \alpha^{52}, \alpha^{62}\right\}, \\
&\quad \left\{0, \alpha^8, \alpha^{16}, \alpha^{25}, \alpha^{55}, \alpha^{56}, \alpha^{59}, \alpha^{61}\right\}\Big\}, \\
C_H\left(\alpha^2 V\right) &:= \left\{\alpha^{9i+2}V : 0 \leq i \leq 6\right\} \\
&= \Big\{\left\{0, \alpha^2, \alpha^3, \alpha^6, \alpha^8, \alpha^{18}, \alpha^{26}, \alpha^{35}\right\}, \left\{0, \alpha^{11}, \alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^{27}, \alpha^{35}, \alpha^{44}\right\}, \\
&\quad \left\{0, \alpha^{20}, \alpha^{21}, \alpha^{24}, \alpha^{26}, \alpha^{36}, \alpha^{44}, \alpha^{53}\right\}, \left\{0, \alpha^{29}, \alpha^{30}, \alpha^{33}, \alpha^{35}, \alpha^{45}, \alpha^{53}, \alpha^{62}\right\}, \\
&\quad \left\{0, \alpha^8, \alpha^{38}, \alpha^{39}, \alpha^{42}, \alpha^{44}, \alpha^{54}, \alpha^{62}\right\}, \left\{0, 1, \alpha^8, \alpha^{17}, \alpha^{47}, \alpha^{48}, \alpha^{51}, \alpha^{53}\right\}, \\
&\quad \left\{0, \alpha^9, \alpha^{17}, \alpha^{26}, \alpha^{56}, \alpha^{57}, \alpha^{60}, \alpha^{62}\right\}\Big\}, \\
C_H\left(\alpha^3 V\right) &:= \left\{\alpha^{9i+3}V : 0 \leq i \leq 6\right\} \\
&= \Big\{\left\{0, \alpha^3, \alpha^4, \alpha^7, \alpha^9, \alpha^{19}, \alpha^{27}, \alpha^{36}\right\}, \left\{0, \alpha^{12}, \alpha^{13}, \alpha^{16}, \alpha^{18}, \alpha^{28}, \alpha^{36}, \alpha^{45}\right\}, \\
&\quad \left\{0, \alpha^{21}, \alpha^{22}, \alpha^{25}, \alpha^{27}, \alpha^{37}, \alpha^{45}, \alpha^{54}\right\}, \left\{0, 1, \alpha^{30}, \alpha^{31}, \alpha^{34}, \alpha^{36}, \alpha^{46}, \alpha^{54}\right\}, \\
&\quad \left\{0, 1, \alpha^9, \alpha^{39}, \alpha^{40}, \alpha^{43}, \alpha^{45}, \alpha^{55}\right\}, \left\{0, \alpha^1, \alpha^9, \alpha^{18}, \alpha^{48}, \alpha^{49}, \alpha^{52}, \alpha^{54}\right\}, \\
&\quad \left\{0, 1, \alpha^{10}, \alpha^{18}, \alpha^{27}, \alpha^{57}, \alpha^{58}, \alpha^{61}\right\}\Big\} \ \ e \\
C_H\left(\alpha^4 V\right) &:= \left\{\alpha^{9i+4}V : 0 \leq i \leq 6\right\} \\
&= \Big\{\left\{0, \alpha^4, \alpha^5, \alpha^8, \alpha^{10}, \alpha^{20}, \alpha^{28}, \alpha^{37}\right\}, \left\{0, \alpha^{13}, \alpha^{14}, \alpha^{17}, \alpha^{19}, \alpha^{29}, \alpha^{37}, \alpha^{46}\right\}, \\
&\quad \left\{0, \alpha^{22}, \alpha^{23}, \alpha^{26}, \alpha^{28}, \alpha^{38}, \alpha^{46}, \alpha^{55}\right\}, \left\{0, \alpha^1, \alpha^{31}, \alpha^{32}, \alpha^{35}, \alpha^{37}, \alpha^{47}, \alpha^{55}\right\}, \\
&\quad \left\{0, \alpha^1, \alpha^{10}, \alpha^{40}, \alpha^{41}, \alpha^{44}, \alpha^{46}, \alpha^{56}\right\}, \left\{0, \alpha^2, \alpha^{10}, \alpha^{19}, \alpha^{49}, \alpha^{50}, \alpha^{53}, \alpha^{55}\right\}, \\
&\quad \left\{0, \alpha^1, \alpha^{11}, \alpha^{19}, \alpha^{28}, \alpha^{58}, \alpha^{59}, \alpha^{62}\right\}\Big\}.
\end{aligned}
$$

Seguindo o que foi feito no Exemplo 4.1.33, novamente, na Tabela 4 *adotamos a notação* α^i *para representar o subespaço vetorial* $\alpha^i V$.

$\mathrm{d}_S(.,.)$	α^1	α^{10}	α^{19}	α^{28}	α^{37}	α^{46}	α^{55}
α^0	4	4	6	6	6	4	6

$\mathrm{d}_S(.,.)$	α^2	α^{11}	α^{20}	α^{29}	α^{38}	α^{47}	α^{56}
α^0	4	6	4	4	6	4	6

$\mathrm{d}_S(.,.)$	α^3	α^{12}	α^{21}	α^{30}	α^{39}	α^{48}	α^{57}
α^0	4	4	6	4	4	4	4

$\mathrm{d}_S(.,.)$	α^4	α^{12}	α^{21}	α^{30}	α^{39}	α^{48}	α^{57}
α^0	4	6	6	4	4	6	4

Tabela 4 – Conjuntos interdistância $D\left(\{V\}, C_H\left(\alpha^i V\right)\right)$, onde $1 \leq i \leq 4$

Portanto, a distância de subespaço mínima de $C_{\langle\alpha\rangle}(V)$ *é 4, a mesma distância de*

subespaço mínima obtida em (ETZION, 2011, Example 1). Foram necessários somente 28 cálculos para encontrar este valor, quantidade bastante inferior aos 63 cálculos necessários para obter o mesmo valor via o método tradicional.

4.1.3 Procedimento de Decodificação Usando Regiões de Voronoi

Nesta subseção apresentamos um procedimento de decodificação para códigos de órbita usando regiões de Voronoi. Como foi feito nas seções anteriores, denote α um dos elementos primitivos de $\mathbb{F}_{q^n}$, visto como um espaço vetorial $n-$dimensional.

O seguinte resultado já foi enunciado no Capítulo 3 (Lema 3.2.20) e é uma adaptação do seu análogo visto na teoria de códigos de bloco.

Lema 4.1.40. *(TRAUTMANN, 2013a) Assuma que a distância de subespaço mínima (ou injeção) de um código de subespaço $C \subset \mathcal{P}_q(n)$ seja δ e $R \in \mathcal{P}_q(n)$ uma palavra recebida. Se existe $U \in C$ cuja distância de R é, no máximo, $\left\lfloor \frac{(d-1)}{2} \right\rfloor$, então U é a única palavra código mais próxima e o decodificador sempre decodificará R como U.*

Com base nos Teorema 4.1.16 e Lema 4.1.40, propomos usar o fato de que todas as regiões de Voronoi de um código de órbita $C_G(V)$ são mutuamente congruentes, e que a partir de uma única região de Voronoi é possível descrever todas as outras, para apresentarmos um procedimento de decodificação para tais códigos. A proposta é baseada nos seguintes passos:

(i) Calcule a região de Voronoi $R_V(V)$ de $V \in \mathcal{G}_q(n,k)$ (ponto inicial da órbita);

(ii) Descreva todas as regiões de Voronoi a partir de $R_V(V)$, conforme é afirmado no Teorema 4.1.16, isto é, dado qualquer $g \in G$, então $R_V(gV) = g\left(R_V(V)\right)$;

(iii) Seja $R \in \mathcal{G}_q(n,k)$ uma palavra recebida pelo decodificador tal que as condições do Lema 4.1.40 são satisfeitas. Encontre a região de Voronoi a que R pertence;

(iv) Decodifique R como o centro da região de Voronoi descrita no passo (iii).

Observação 4.1.41. *Ao contrário do que foi feito no procedimento de decodificação via síndromes proposto em (TRAUTMANN F. MANGANIELLO, 2013), não precisamos calcular os quocientes associados às órbitas nem a aplicação canonizadora.*

A seguir apresentamos um exemplo do procedimento de decodificação via regiões de Voronoi.

Para $q = p$ primo, dada a ação de um subgrupo de $P\Gamma L_n(\mathbb{F}_q)$ sobre $\mathcal{G}_q(n,k)$, como a definição de órbita está relacionada com classes de equivalência (ROTMAN, 1995,

pag.56) em $\mathcal{G}_q(n,k)$, particionaremos a grassmanniana $\mathcal{G}_q(n,k)$ considerando a ação do grupo $\langle\alpha\rangle \rtimes \langle\sigma\rangle$ sobre ela, isto é, o produto semi-direto do grupo cíclico gerado por um elemento primitivo α de $\mathbb{F}_{q^n}$ e o grupo (cíclico) de automorfismos de $\mathbb{F}_{q^n}$, o qual é gerado pelo automorfismo de Frobenius $\sigma(x) = x^q$, para todo $x \in \mathbb{F}_{q^n}$. Escolhemos este grupo, pois ele reduz o número de órbitas e ainda oferece uma forma simples de descrever os subespaços $k-$dimensionais que compõe $\mathcal{G}_q(n,k)$.

Exemplo 4.1.42. *Sejam $p(x) = x^6 + x + 1 \in \mathbb{F}_2[x]$ um polinômio primitivo e $\alpha \in \mathbb{F}_{2^6} \simeq \mathbb{F}_2[x]/\langle p(x)\rangle$ uma raiz de $p(x)$. A grassmanniana $\mathcal{G}_2(6,3)$ pode ser particionada como*

$$\mathcal{G}_2(6,3) = \left\{ \bigcup_{i=1}^{6} C_{\langle\alpha\rangle\rtimes\langle\sigma\rangle}(V_i) \right\} \cup C_{\langle\alpha\rangle}(\mathbb{F}_{2^3}), \tag{4.32}$$

onde $\mathbb{F}_{2^3} = \{0, 1, \alpha^9, \alpha^{18}, \alpha^{27}, \alpha^{36}, \alpha^{45}, \alpha^{54}\}$ e

$$\begin{aligned}
V_1 &:= \left\{0, 1, \alpha, \alpha^2, \alpha^6, \alpha^7, \alpha^{12}, \alpha^{26}\right\}, \\
V_2 &:= \left\{0, 1, \alpha, \alpha^4, \alpha^6, \alpha^{16}, \alpha^{24}, \alpha^{33}\right\}, \\
V_3 &:= \left\{0, \alpha^7, \alpha^{16}, \alpha^{18}, \alpha^{28}, \alpha^{32}, \alpha^{49}, \alpha^{52}\right\}, \\
V_4 &:= \left\{0, \alpha, \alpha^3, \alpha^{12}, \alpha^{13}, \alpha^{18}, \alpha^{26}, \alpha^{48}\right\}, \\
V_5 &:= \left\{0, \alpha, \alpha^{18}, \alpha^{22}, \alpha^{29}, \alpha^{42}, \alpha^{43}, \alpha^{48}\right\} \text{ e} \\
V_6 &:= \left\{0, \alpha^4, \alpha^{17}, \alpha^{26}, \alpha^{39}, \alpha^{54}, \alpha^{61}, \alpha^{62}\right\}.
\end{aligned} \tag{4.33}$$

Observe que $\left|C_{\langle\alpha\rangle\rtimes\langle\sigma\rangle}(V_j)\right| = 378$, para $j \in \{1,4\}$, isto é, esses códigos possuem estabilizadores triviais. Por outro lado, $\left|C_{\langle\alpha\rangle\rtimes\langle\sigma\rangle}(V_j)\right| = 126$, para $j \in \{2,5\}$, e $\left|C_{\langle\alpha\rangle\rtimes\langle\sigma\rangle}(V_j)\right| = 189$, para $j \in \{3,6\}$, onde os estabilizadores destas órbitas têm ordens 3 e 2, respectivamente. Assim, somando as cardinalidades dos códigos $C_{\langle\alpha\rangle\rtimes\langle\sigma\rangle}(V_j)$, para $1 \leq j \leq 6$, obtemos 1386 subespaços 3-dimensionais. Além disso, somando a cardinalidade do código spread $C_{\langle\alpha\rangle}(\mathbb{F}_{2^3})$, obtemos um total de 1395 subespaços 3-dimensionais/palavras, que é precisamente a cardinalidade da grassmanniana $\mathcal{G}_2(6,3)$ (Ver Equação (2.32)).

Considere o $(6,9,6,3)$-código de subespaço (geometricamente uniforme) $C_{\langle\alpha\rangle}(\mathbb{F}_{2^3})$. De acordo com o Teorema 4.1.16, para descrevermos todas as regiões de Voronoi deste código, basta apenas uma única região de Voronoi (Definição 4.1.14), pois as demais são obtidas a partir do grupo $\langle\alpha\rangle$, gerador do código de órbita em questão. Assim, considerando a região de Voronoi centrada na palavra código/ponto inicial (corpo finito) $\mathbb{F}_{2^3}$, obtemos

$$\begin{aligned}
R_V(\mathbb{F}_{2^3}) := \big\{ & \alpha^3 V_2, \alpha^{12} V_2, \alpha^{21} V_2, \alpha^{30} V_2, \alpha^{39} V_2, \alpha^{48} V_2, \alpha^{57} V_2, \\
& \alpha^6 \sigma(V_2), \alpha^{15} \sigma(V_2), \alpha^{24} \sigma(V_2), \alpha^{33} \sigma(V_2), \alpha^{42} \sigma(V_2), \alpha^{51} \sigma(V_2), \alpha^{60} \sigma(V_2), \\
& \alpha^2 V_3, \alpha^{11} V_3, \alpha^{20} V_3, \alpha^{29} V_3, \alpha^{38} V_3, \alpha^{47} V_3, \alpha^{56} V_3, \\
& \alpha^4 \sigma(V_3), \alpha^{13} \sigma(V_3), \alpha^{22} \sigma(V_3), \alpha^{31} \sigma(V_3), \alpha^{40} \sigma(V_3), \alpha^{49} \sigma(V_3), \alpha^{58} \sigma(V_3),
\end{aligned} \tag{4.34}$$

$$\alpha^8\sigma^2\left(V_3\right),\alpha^{17}\sigma^2\left(V_3\right),\alpha^{26}\sigma^2\left(V_3\right),\alpha^{35}\sigma^2\left(V_3\right),\alpha^{44}\sigma^2\left(V_3\right),\alpha^{53}\sigma^2\left(V_3\right),$$
$$\alpha^{62}\sigma^2\left(V_3\right),$$
$$\alpha^6V_4,\alpha^{15}V_4,\alpha^{24}V_4,\alpha^{33}V_4,\alpha^{42}V_4,\alpha^{51}V_4,\alpha^{60}V_4,$$
$$\alpha^3\sigma\left(V_4\right),\alpha^{12}\sigma\left(V_4\right),\alpha^{21}\sigma\left(V_4\right),\alpha^{30}\sigma\left(V_4\right),\alpha^{39}\sigma\left(V_4\right),\alpha^{48}\sigma\left(V_4\right),\alpha^{57}\sigma\left(V_4\right),$$
$$\alpha^6\sigma^2\left(V_4\right),\alpha^{15}\sigma^2\left(V_4\right),\alpha^{24}\sigma^2\left(V_4\right),\alpha^{33}\sigma^2\left(V_4\right),\alpha^{42}\sigma^2\left(V_4\right),\alpha^{51}\sigma^2\left(V_4\right)$$
$$\alpha^{60}\sigma^2\left(V_4\right),$$
$$\alpha^3\sigma^3\left(V_4\right),\alpha^{12}\sigma^3\left(V_4\right),\alpha^{21}\sigma^3\left(V_4\right),\alpha^{30}\sigma^3\left(V_4\right),\alpha^{39}\sigma^3\left(V_4\right),\alpha^{48}\sigma^3\left(V_4\right)$$
$$\alpha^{57}\sigma^3\left(V_4\right),$$
$$\alpha^6\sigma^4\left(V_4\right),\alpha^{15}\sigma^4\left(V_4\right),\alpha^{24}\sigma^4\left(V_4\right),\alpha^{33}\sigma^4\left(V_4\right),\alpha^{42}\sigma^4\left(V_4\right),\alpha^{51}\sigma^4\left(V_4\right)$$
$$\alpha^{60}\sigma^4\left(V_4\right),$$
$$\alpha^3\sigma^5\left(V_4\right),\alpha^{12}\sigma^5\left(V_4\right),\alpha^{21}\sigma^5\left(V_4\right),\alpha^{30}\sigma^5\left(V_4\right),\alpha^{39}\sigma^5\left(V_4\right),\alpha^{48}\sigma^5\left(V_4\right)$$
$$\alpha^{57}\sigma^5\left(V_4\right),$$
$$\alpha V_6,\alpha^{10}V_6,\alpha^{19}V_6,\alpha^{28}V_6,\alpha^{37}V_6,\alpha^{46}V_6,\alpha^{55}V_6,$$
$$\alpha^2\sigma\left(V_6\right),\alpha^{11}\sigma\left(V_6\right),\alpha^{20}\sigma\left(V_6\right),\alpha^{29}\sigma\left(V_6\right),\alpha^{38}\sigma\left(V_6\right),\alpha^{47}\sigma\left(V_6\right),\alpha^{56}\sigma\left(V_6\right),$$
$$\alpha^4\sigma^2\left(V_6\right),\alpha^{13}\sigma^2\left(V_6\right),\alpha^{22}\sigma^2\left(V_6\right),\alpha^{31}\sigma^2\left(V_6\right),\alpha^{40}\sigma^2\left(V_6\right),\alpha^{49}\sigma^2\left(V_6\right)$$
$$\alpha^{58}\sigma^2\left(V_6\right)\Big\}$$

onde, dado o subespaço vetorial k*-dimensional* $V_t=\left\{0,\alpha^{i_1},...,\alpha^{i_{q^k-1}}\right\}$*, o subespaço vetorial* k*-dimensional* $\alpha^j\sigma^i\left(V_t\right)$ *é descrito como* $\alpha^j\sigma^i\left(V_t\right)=\left\{0,\alpha^j\sigma^i\left(\alpha^{i_1}\right),...,\alpha^j\sigma^i\left(\alpha^{i_{q^k-1}}\right)\right\}$.

A região de Voronoi $R_V\left(\mathbb{F}_{2^3}\right)$ *possui 98 palavras de* $\mathcal{G}_2(6,3)$*, ou seja,* $\left|R_V\left(\mathbb{F}_{2^3}\right)\right|=98$*. Mais ainda, como* $\mathcal{G}_2(6,3)$ *é um código (trivial) de órbita gerado pela ação do grupo* $P\Gamma L_6\left(\mathbb{F}_2\right)$ *sobre qualquer subespaço vetorial* 3*-dimensional* W *então, pelo Teorema 4.1.16, o perfil de distância global* $DP\left(\mathcal{G}_2(6,3)\right)$ *é*

$$\begin{aligned} DP\left(\mathcal{G}_2(6,3)\right) &= 512 \text{ palavras cuja a distância para } W \text{ é igual a } 6, \\ &= 784 \text{ palavras cuja a distância para } W \text{ é igual a } 4, \\ &= 98 \text{ palavras cuja a distância para } W \text{ é igual a } 2. \end{aligned} \tag{4.35}$$

Para o uso do procedimento de decodificação baseado nas regiões de Voronoi aqui apresentado, é necessário a descrição completa do grupo de simetrias que age sobre o código. Como o grupo de simetrias (e grupo gerador) de $C_{\langle\alpha\rangle}\left(\mathbb{F}_{2^3}\right)$ *é o grupo cíclico* $\langle\alpha\rangle$ *(ou o grupo cíclico* $\langle M_p\rangle$ *quando consideramos subespaços vetoriais em* $\mathbb{F}_2^6$*), então todas as regiões de Voronoi são calculadas como* $\alpha^i\left(R_V\left(\mathbb{F}_{2^3}\right)\right)=\left\{\alpha^iU:U\in R_V\left(\mathbb{F}_{2^3}\right)\right\}$*, para* $0\leq i\leq 8$.

De acordo com o Lema 4.1.40, podemos corrigir todas as palavras cuja distância para as palavras código de $C_{\langle\alpha\rangle}\left(\mathbb{F}_{2^3}\right)$ *sejam iguais a* 2*. Logo, suponha que as palavras* $R_1=\alpha^8\sigma^4\left(V_4\right)$ *e* $R_2=\alpha^{19}\sigma^5\left(V_4\right)$ *sejam recebidas pelo decodificador. Como* $R_1=\alpha^2\left[\alpha^6\sigma^4\left(V_4\right)\right]$

e $R_2 = \alpha^7\left[\alpha^{12}\sigma^5\left(V_4\right)\right]$*, onde* $\alpha^6\sigma^4\left(V_4\right)$ *e* $\alpha^{12}\sigma^5\left(V_4\right)$ *pertencem a* $R_V\left(\mathbb{F}_{2^3}\right)$ *(Ver Equação (4.34)), logo* $R_1 \in \alpha^2\left(R_V\left(\mathbb{F}_{2^3}\right)\right)$ *e* $R_2 \in \alpha^7\left(R_V\left(\mathbb{F}_{2^3}\right)\right)$*, e então estas palavras são unicamente decodificadas como* $\alpha^2\mathbb{F}_{2^3}$ *e* $\alpha^7\mathbb{F}_{2^3}$*, respectivamente.*

Observação 4.1.43. *É possível aplicar o procedimento de decodificação proposto nesta subseção a procedimentos de decodificação de lista (Ver Definição 3.2.21).*

4.2 Construção Multinível Aplicada a Códigos de Órbita

Construções multiníveis foram, pela primeira vez, aplicadas no contexto de códigos de subespaço na tese de (NóBREGA, 2009), onde o autor propõe uma construção multinível para códigos de subespaço m-shot. Neste trabalho, aplicaremos esta construção multinível para códigos de órbita, considerando uma cadeia de partições geometricamente uniformes.

As principais referências desta seção são (CALDERBANK, 1989; NóBREGA, 2009; UNGERBOECK, 1982).

4.2.1 Particionamento de Conjuntos

Assim como nas outras subseções, denote (M, d) um espaço métrico e $C \subset (M, d)$ um código. Seja $C_1 \subset C$ tal que seja possível obter uma partição $C/C_1 = \{C_1, C_{11}, ..., C_{1t_1}\}$ de C. O número $|C/C_1| = t_1 + 1$ é dito a ordem da partição. Em particular, se $t_1 + 1 = 2$, então a partição será chamada binária.

Definição 4.2.1. *A distância intrasubconjunto* δ_1 *de* C/C_1 *é definida como*

$$\delta_1 := \min_{C_{1i} \in C/C_1,\ c_1, c_2 \in C_{1i}\ \ e\ c_1 \neq c_2} \left\{d\left(c_1, c_2\right)\right\}. \tag{4.36}$$

Por convenção, se B *é um conjunto unitário, então a distância mínima (ou intrasubconjunto) de* B *é descrita como* $d(B) = \infty$*.*

Definição 4.2.2. *Para* $C_1 = C_{10}$*, a partição* $C/C_1 = \{C_{10}, C_{11}, ..., C_{1t_1}\}$ *é dita equitativa se* $|C_{1i}| = |C_{1j}|$ *e* $d\left(C_{1i}\right) = d\left(C_{1j}\right)$*, para todos* $0 \leq i < j \leq t_1$*.*

O Teorema 4.1.25 garante que as partições $C_{G/H}(V)$ de um código de órbita $C_G(V)$, geradas a partir de um subgrupo $H \lhd G$, são todas equitativas. A definição de partição equitativa é equivalente a Definição 4.1.29 (partição justa) vista em (BIGLIERI, 1988).

Dada uma cadeia de subcódigos $C_m \subset C_{m-1} \subset ... \subset C_1 \subset C_0 = C$, considere agora uma cadeia de partições, que será denotada por $C_0/C_1/.../C_{m-1}/C_m$ onde, por exemplo, cada um dos conjuntos C_{1j} de $C_0/C_1 = \{C_{10}, C_{11}, ..., C_{1t_1}\}$ é refinado pelo conjunto C_2,

de forma que

$$C = C_0/C_1/C_2 = \bigcup_{0\leq j\leq t_1} C_{1j}/C_2. \tag{4.37}$$

Procedendo de forma análoga para os demais níveis da cadeia, assumimos que a partição do $m-1$-ésimo nível $C_0/C_1/.../C_{m-1}$ por C_m corresponde a uma partição de C formada somente por conjuntos unitários.

Uma extensão natural do conceito de partição equitativa (Definição 4.2.2) ocorre quando cada nível de uma cadeia de partições é equitativa e, em cada nível i, todos os subconjuntos daquele nível possuem a mesma distância intrasubconjunto δ_i. Além disso, uma cadeia de partições é chamada binária, se todas as partições envolvidas são binárias.

De agora em diante, consideraremos apenas particionamentos de conjuntos/códigos que satisfazem a seguinte relação

$$\text{Dada } C = C_0/C_1/.../C_{m-1}/C_m, \text{ então } d(C) = \delta_0 \leq \delta_1 \leq ... \leq \delta_{m-1} \leq \delta_m = \infty, \tag{4.38}$$

ou seja, no m-nível, C é particionado por conjuntos unitários, cada um constituído por uma palavra código de C.

De posse destas definições, estamos aptos a descrever o mapeamento por Particionamento de Conjunto:

(i) Seja $C \subset (M, d)$ um código, tal que $|C| = 2^m$;

(ii) De posse de C, considere uma cadeia de partições $C = C_0/C_1/.../C_{m-1}/C_m$ binária e equitativa, que satisfaça (4.38);

(iii) A cada refinamento, rotule os dois subconjuntos de C por 0 ou 1 tal que, no m-ésimo nível, cada elemento $c \in C$ é associado a uma sequência $\chi(c) = (a_1, a_2..., a_m) \in \mathbb{F}_2^m$.

Observação 4.2.3. *Vale destacar que o rotulamento χ não é único.*

Exemplo 4.2.4. *De acordo com a Figura 7, o Particionamento de Conjunto proposto é $\chi(C) = \{00, 01, 10, 11\}$.*

Satisfeitas todas as condições do Particionamento de Conjunto, então enunciamos o Lema 4.2.5, conhecido como Lema da Distância de Partição.

Lema 4.2.5. *(JR., 1988) Considere $C \subset (M, d)$ um código e $C = C_0/C_1/.../C_{m-1}/C_m$ uma cadeia de partições por subcódigos (subconjuntos) de C, cujas distâncias intrasubconjunto δ_i satisfazem (4.38). Se $\chi(c_1) = a = (a_1, a_2, ..., a_M)$ e $\chi(c_2) = b = (b_1, b_2, ..., b_M)$ são os rótulos das palavras código $c_1, c_2 \in C$, respectivamente, então*

$$d(a, b) \geq \delta_j, \text{ onde } j = \min_{0\leq i<M} \{i : a_i \neq b_i\}. \tag{4.39}$$

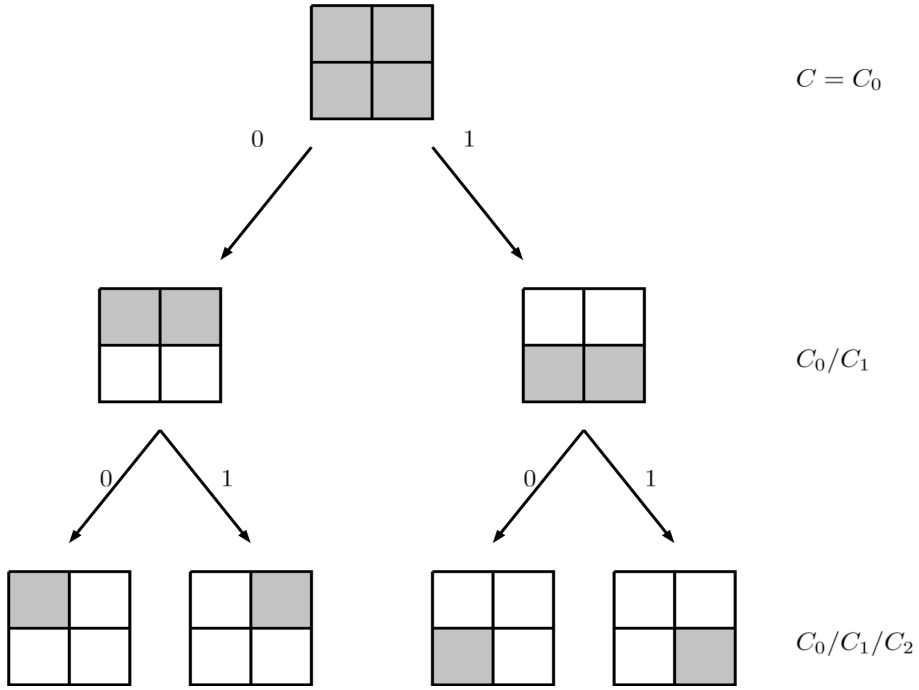


Figura 7 – Particionamento de Conjunto para um código C, tal que $|C| = 4$

O rotulamento por Particionamento de Conjunto é restritivo, uma vez que exigi-se que as partições sejam binárias. Esta condição restringe, por exemplo, à aplicação de tal rotulamento para um código de órbita $C_{\langle\alpha\rangle}(V)$, onde V é um subespaço k-dimensional de $\mathbb{F}_{2^n}$ e $\alpha \in \mathbb{F}_{2^n} \simeq \mathbb{F}_2[x]/\langle p(x)\rangle$ é uma raiz do polinômio primitivo $p(x) \in \mathbb{F}_2[x]$ de grau n, uma vez que $\left|C_{\langle\alpha\rangle}(V)\right| = 2^n - 1$ é um número ímpar.

4.2.2 Codificação Multinível - Calderbank

O rotulamento proposto por Calderbank (CALDERBANK, 1989) pode ser visto como uma generalização do Particionamento de Conjunto, uma vez que não é restrito a partições binárias.

Definição 4.2.6. *Dado um código $C \subset (M, d)$, uma partição aninhada $L-$nível de C é uma cadeia de partições $\Gamma_0, \Gamma_1, ..., \Gamma_L$, onde a partição Γ_i é um refinamento da partição Γ_{i-1}. Interpretando a partição $L-$ nível como um grafo, dado $1 \leq i \leq L-1$, cada subconjunto (vértice) do nível Γ_i esta unido a p_{i+1} subconjuntos de Γ_{i+1}. Além disso, é exigido que cada vértice y no nível Γ_i esteja conectado por uma aresta a um único vértice x no nível Γ_{i-1}, assim como cada vértice z no nível Γ_{i+1} esteja conectado por uma aresta a um único vértice x no Γ_i-ésimo nível.*

Observação 4.2.7. *Durante todo esta subseção, consideraremos apenas partições L-nível aninhadas.*

Cada aresta que conecta o nível Γ_i ao nível Γ_{i+1} será rotulada com um dos números

$0, 1, 2, ..., p_{i+1} - 1$. Além disso, o grau de um vértice (quantidade de subconjuntos ligados a ele) pode variar de um nível para o outro. Assim, para algum $1 \leq i \leq L$, dado $S \in \Gamma_i$ um subconjunto de C, este subconjunto pode ser rotulado por uma sequência $(a_1, a_2, ..., a_i)$, que aponta a correspondente posição de S na partição L-nível.

Exemplo 4.2.8. *A Figura 8 a seguir exemplifica uma partição* 2*-nível aninhada de um conjunto de vinte elementos.*

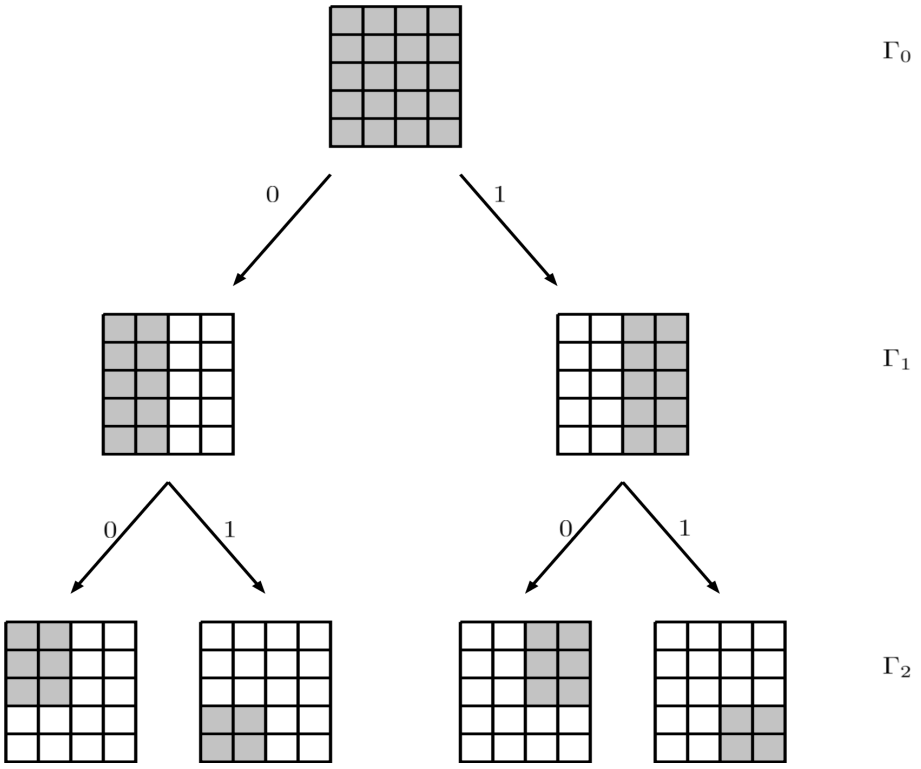


Figura 8 – Partição 2-nível

Os subconjuntos S_1, S_2, S_3 *e* S_4 *do nível* 2 *podem ser rotulados como* 00*,* 01*,* 10 *e* 11*, respectivamente. Tal rotulamento, de fato, generaliza o Particionamento de Conjunto.*

Definição 4.2.9. *Dado* $C \subset (M, d)$*, onde* $S_1, S_2 \subset C$*, a distância intersubconjunto é definida como*

$$d(S_1, S_2) := \min_{a \in S_1, b \in S_2} \{d(a, b)\}. \tag{4.40}$$

O desafio agora é buscar um rotulamento para os subconjuntos/subcódigos de C ou, em particular, para as palavras código de C, de forma que possamos garantir uma proteção maior para a transmissão da informação do que aquela já oferecida por C.

De agora em diante, dado C um código, considere uma partição L-nível de C com distâncias intrasubconjunto satisfazendo (4.38).

Definição 4.2.10. *Um código L-nível* $\mathcal{C} = [\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_L]$ *onde, para todo* $1 \leq i \leq L$*, os códigos componentes* $\mathcal{C}_i$ *utilizam* $\{0, 1, 2, ..., p_i - 1\}$ *como alfabeto, é formado por sequências* $\left(a_1^k, a_2^k, ..., a_L^k\right)$*, tais que* $a_i^k \in \mathcal{C}_i$*.*

Observação 4.2.11. *Utilizaremos códigos no espaço de Hamming* $\left(\mathbb{F}_q^N, d_H\right)$ *como códigos componentes, e todos os códigos devem possuir o mesmo comprimento.*

Dada a distância intrasubconjunto δ_L, o código L-nível $\mathcal{C}$ deve ser escolhido de tal forma que $\delta_L \geq d_H(\mathcal{C})$. Além disso, a distância mínima $d_H(\mathcal{C}_i)$ de todo código componente deve satisfazer $d_H(\mathcal{C}_i)\,\delta_i \geq d_H(\mathcal{C})$. Então, assim como ocorre na codificação multinível proposta em (IMAI, 1977), tem-se

$$d(\mathcal{C}) = \min\left\{d_H(\mathcal{C}_1)\,\delta_0, d_H(\mathcal{C}_2)\,\delta_1, ..., d_H(\mathcal{C}_L)\,\delta_{L-1}, \delta_L\right\}. \tag{4.41}$$

Exemplo 4.2.12. *(NóBREGA, 2009) Considere o código de subespaço* $C = \mathcal{P}_2(3)$*. Logo*

$$C = \mathcal{P}_2(3) = \left\{\{0\}, V_1, V_2, ..., V_7, V_1^\perp, V_2^\perp, ..., V_7^\perp, \mathbb{F}_2^3\right\} \tag{4.42}$$

onde, para cada $1 \leq i \leq 7$*,* V_i *corresponde a um dos subespaços unidimensionais de* $\mathbb{F}_2^3$*, e* $V_i^\perp$ *o respectivo complemento ortogonal. O código* C *admite a seguinte partição* $2-$*nível*

$$\begin{aligned}
\Gamma_0 &= \left\{\{0\}, V_1, V_2, ..., V_7, V_1^\perp, V_2^\perp ..., V_7^\perp, \mathbb{F}_2^3\right\} = C \\
\Gamma_1 &= \left\{\{\{0\}, V_1, V_2, ..., V_7\}, \left\{V_1^\perp, V_2^\perp, ..., V_7^\perp \mathbb{F}_2^3\right\}\right\} \\
\Gamma_2 &= \left\{\{0\}, \{V_1\}, \{V_2\}, ..., \{V_7\}, \left\{V_1^\perp\right\}, \left\{V_2^\perp\right\}, ..., \left\{V_7^\perp\right\} \left\{\mathbb{F}_2^3\right\}\right\},
\end{aligned}$$

onde $\delta_0 = 1$*,* $\delta_1 = 2$ *e* $\delta_2 = \infty$*.*

Como $d_S(C) = 1$ *e* $\delta_2 \geq 3$*, é possível utilizar codificação multinível, de forma a obter um novo código com distância mínima três. Considere os códigos componentes* $\mathcal{C}_1 = \{(000), (111)\}$ *(binário, pois* Γ_1 *é um refinamento de* Γ_0 *a partir de dois conjuntos) e* $\mathcal{C}_2 = \{(000), (017), (026), ..., (772)\}$ *(octal, pois* Γ_2 *é um refinamento de cada elemento de* Γ_1 *a partir de oito conjuntos). Assim* $\mathcal{C} = [\mathcal{C}_1, \mathcal{C}_2]$ *é um código* $2-$*nível, ilustrado na Figura 9, onde* $d_H(\mathcal{C}_1) = 3$ *e* $d_H(\mathcal{C}_2) \geq \frac{3}{2}$ *e, portanto,*

$$d(\mathcal{C}) = \min\left\{d_H(C_1)\,\delta_0, d_H(C_2)\,\delta_1\right\} = 3. \tag{4.43}$$

Aplicaremos a técnica de codificação multinível de (CALDERBANK, 1989), adaptada para o contexto de códigos de subespaço por (NóBREGA, 2009), para códigos de órbita $C_G(V)$, onde $G = G_0$, a partir de uma cadeia de partições geometricamente uniformes obtida de uma série normal $G_0 \geq G_1 \geq ... \geq G_m = \{Id_n\}$ de G. Justifica-se o uso de uma cadeia de partições geometricamente uniformes pois, conforme foi visto no

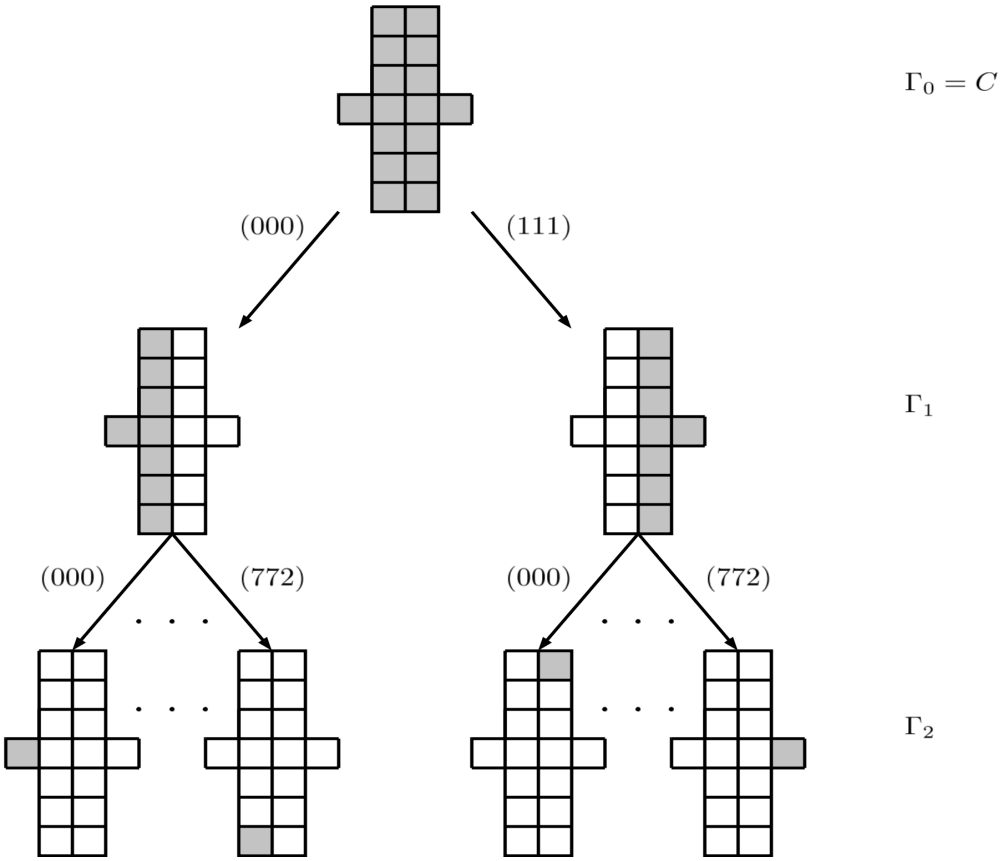


Figura 9 – Código 2−nível C proposto no Exemplo 4.2.12

Teorema 4.1.25, dado um nível i desta partição, que corresponde a sucessivas partições de $C_G(V)$ utilizando a série normal $G = G_0 \geq G_1 \geq ... \geq G_{i-1} \geq G_i$, todos os subcódigos neste nível possuem a mesma distância de subespaço intrasubconjunto, a qual é exatamente a distância de subespaço mínima neste nível. Este fato reduz drasticamente a quantidade de cálculos necessários para a obtenção de δ_i. Além disso, todos os subcódigos possuem a mesma cardinalidade, pois têm o mesmo grupo gerador e, portanto, para cada refinamento no nível $i+1$, tem-se uma nova partição de $C_G(V)$ aninhada, para todo $1 \leq i \leq m-1$.

Exemplo 4.2.13. *Sejam $p(x) = x^6 + x + 1 \in \mathbb{F}_2[x]$ um polinômio primitivo, $\alpha \in \mathbb{F}_{2^6} \simeq \mathbb{F}_2[x]/\langle p(x)\rangle$ uma raiz de $p(x)$ e $V = \{0, 1, \alpha^8, \alpha^{10}, \alpha^{20}, \alpha^{48}, \alpha^{59}, \alpha^{61}\}$ um subespaço 3 dimensional de $\mathbb{F}_{2^6}$. Assim como foi feito no Exemplo 4.1.31, considere a série de composição $\langle\alpha\rangle > \langle\alpha^3\rangle > \langle\alpha^9\rangle$, tal que*

$$C_{\langle\alpha\rangle}(V) = \bigcup_{i=0}^{2} C_{\langle\alpha^3\rangle}\left(\alpha^i V\right) = \bigcup_{i=0}^{8} C_{\langle\alpha^9\rangle}\left(\alpha^i V\right). \tag{4.44}$$

Conforme já foi comentado, é direto observar que uma cadeia de partições geometricamente uniformes de um código de órbita $C_G(V)$ é uma partição $L-$nível (aninhada), onde L está relacionado como o comprimento de uma dada série normal de G. Assim,

retornando ao código de órbita $C_{\langle\alpha\rangle}(V)$, é verificado (Teorema 4.1.25) que a distância intrasubconjunto no nível 1 é igual a distância mínima de qualquer um dos subcódigos de órbita que compõe tal nível. Logo $\delta_1 = d_S\left(C_{\langle\alpha^3\rangle}\left(\alpha^i V\right)\right) = 2$, para $i = \{0,1,2\}$. Pelo mesmo argumento, no nível 2 a distância intrasubconjunto $\delta_2 = d_S\left(C_{\langle\alpha^9\rangle}\left(\alpha^i V\right)\right) = 6$, para $i = \{0,1,...,8\}$, e no nível 3, que é o refinamento do nível 2 a partir de subconjuntos unitários/palavras código, tem-se a distância intrasubconjunto $\delta_3 = \infty$.

Suponha que desejamos elevar a proteção do código de órbita $C_{\langle\alpha\rangle}(V)$, cuja distância de subespaço mínima é dois $\left(d_S\left(C_{\langle\alpha\rangle}(V)\right) = 2,\ Exemplo\ 4.1.31\right)$, de forma que, a partir de uma codificação multinível, a nova distância mínima seja quatro.

Considere o código $3-$nível $\mathcal{C} = [\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3]$, tal que

$$\begin{aligned}
\mathcal{C}_1 &= \{(000),(111),(222)\} \Rightarrow d_H(\mathcal{C}_1) = 3 \\
\mathcal{C}_2 &= \{(100),(010),(001),(211),(112),(121),(022),(202),(220)\} \Rightarrow d_H(\mathcal{C}_2) = 2 \\
\mathcal{C}_3 &= \{v_1, v_2, ..., v_{63}\} \subset \mathbb{F}_7^3 \Rightarrow d_H(\mathcal{C}_3) \geq 1.
\end{aligned}$$

Com relação a $\mathcal{C}_3$, podemos escolher quaisquer 63 vetores (palavras código) de $\mathbb{F}_7^3$ uma vez que, de acordo com a nova distância mínima proposta (quatro) e por (4.41), $d_H(\mathcal{C}_3)$ não influenciará no resultado. De fato,

$$\begin{aligned}
d(\mathcal{C}) &= \min\{\delta_0 d_H(\mathcal{C}_1), \delta_1 d_H(\mathcal{C}_2), \delta_2 d_H(\mathcal{C}_3), \delta_3\} \\
&= \min\{2.3, 2.2, 6 d_H(\mathcal{C}_3)\} \\
&= 4.
\end{aligned}$$

As palavras código de $C_{\langle\alpha\rangle}(V)$ podem ser rotuladas da forma apresentada na Figura 10.

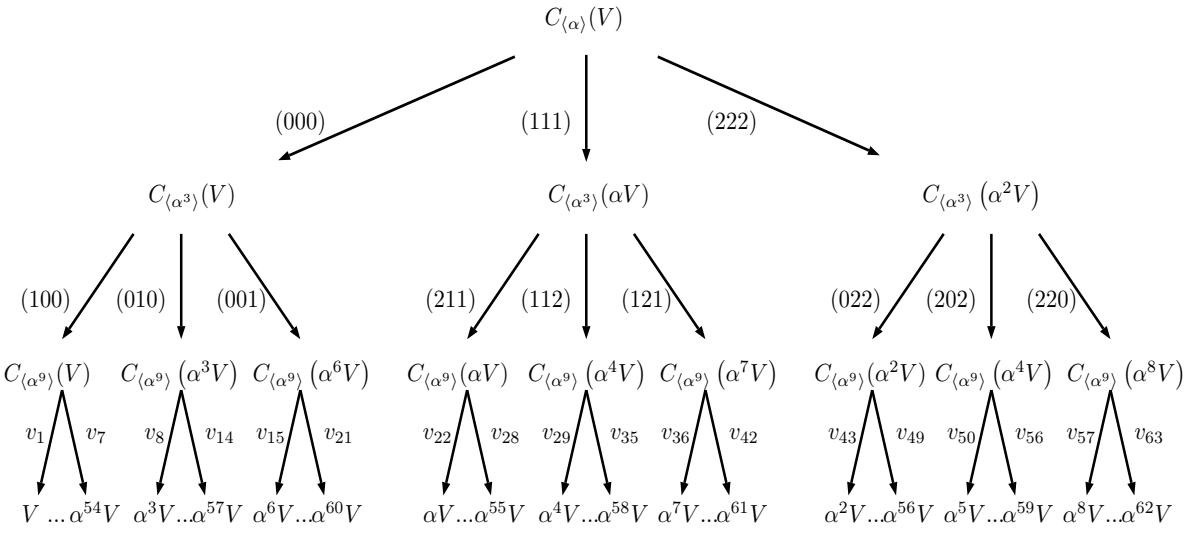


Figura 10 – Codificação multinível aplicada a $C_{\langle\alpha\rangle}(V)$

Se, por exemplo, considerarmos $v_1 = (000), v_2 = (111), v_3 = (222) \in \mathbb{F}_7^3$*, então as palavras código* V*,* $\alpha^9 V$ *e* $\alpha^{18} V$ *podem ser rotuladas como*

$$\begin{array}{rcl} V & \mapsto & 000100000 \\ \alpha^9 V & \mapsto & 000100111 \\ \alpha^{18} V & \mapsto & 000100222. \end{array} \tag{4.45}$$

4.3 Comentários Finais

Na primeira parte deste capítulo, verificamos que existe uma equivalência entre códigos de órbita e códigos geometricamente uniformes, que por sua vez também podem ser vistos como códigos casados a grupos. Logo, em $\mathcal{G}_q(n,k)$, não há diferença entre essas três famílias de códigos. Tais equivalências foram obtidas, principalmente, a partir de uma análise da literatura sobre o grupo de isometrias que age em $\mathcal{P}_q(n)$.

De posse da equivalência entre códigos de órbita e códigos geometricamente uniformes, buscamos explorar os particionamentos dos códigos de órbita obtidos a partir da ação de grupos quocientes sobre o ponto inicial da órbita. Para isso, foi necessário enunciarmos um resultado que descreve sobre quais condições um dado subgrupo de $GL_n(\mathbb{F}_q)$ admite um subgrupo normal não trivial. Também apresentamos a definição de séries normais e um exemplo de como obter diversos refinamentos de uma partição geometricamente uniforme.

Dado o completo entendimento sobre partições geometricamente uniformes, pudemos explorá-las a fim de obtermos alguns resultados interessantes para um melhor uso dos códigos de órbita no contexto de codificação de redes lineares aleatórias. Em primeiro lugar, para códigos de órbita gerados a partir de subgrupos abelianos de $GL_n(\mathbb{F}_q)$, e aqui se inclui a classe dos códigos de órbita cíclicos, observamos que é possível reduzir consideravelmente o número de operações necessárias para a obtenção da distância mínima destes códigos. Ainda, apresentamos, com base na classificação dos códigos de órbita como geometricamente uniformes, um algoritmo de decodificação bastante simples, que faz uso, basicamente, do grupo gerador de tais códigos.

Por outro lado, obtemos uma forma sistemática para a aplicação de codificação multinível a códigos de órbita. Dada uma cadeia de partições obtida por uma série normal do grupo gerador da órbita, basta calcularmos a distância mínima de um único subcódigo de órbita de um dado nível para obtermos a distância intrasubconjunto deste nível. Isso, novamente, reduz a quantidade de operações necessárias para a obtenção da distância mínima de um código $L-$nível.

Por fim, concluímos este capítulo observando o fato de que códigos de órbita serem geometricamente uniformes abre uma grande oportunidade de construção de bons (com respeito aos parâmetros e/ou algoritmos de decodificação) códigos de subespaço, uma vez

que esta classe de códigos alia uma estrutura geométrica muito sólida com uma estrutura algébrica bastante conhecida. No capítulo de Conclusões comentaremos mais sobre possibilidades de pesquisa decorrentes da equivalência proposta neste capítulo.

5 Codificação de Redes Quânticas

Neste capítulo, apresentamos uma proposta inovadora, do ponto de vista teórico, de uma hipotética rede de transmissão de informações quânticas que admite codificação. Esta rede, e os princípios que a norteiam, são embasados na codificação de redes lineares vista no Capítulo 3. Para esta proposta, devemos analisar como a informação quântica é descrita em função dos pacotes de informações clássicas enviados por uma fonte, como os possíveis nós intermediários de uma rede quântica podem processar as informações recebidas de outros nós, etc.

Para um entendimento inicial deste problema de pesquisa, na Seção 5.1 abordamos alguns conceitos iniciais de mecânica quântica, necessários para a definição e descrição de uma possível rede quântica. Gostaríamos de frisar que a mecânica quântica é uma ampla área de pesquisa, recente se comparada com outros tópicos da física, e que ainda não é totalmente compreendida até mesmo entre os mais renomados pesquisadores. Nosso objetivo nesta seção baseia-se simplesmente na definição matemática de itens necessários para o desenvolvimento deste trabalho.

Já na Seção 5.2, apresentamos uma definição do fenômeno físico conhecido como emaranhamento quântico. Dizemos “uma definição", pois conforme explicitaremos, este fenômeno físico ainda não é bem compreendido e pode ser definido de diferentes formas. Para os problemas relacionados à computação e teoria da informação quânticas, este fenômeno é essencial para o desenvolvimento em alta performance dos cálculos, bem como para a proteção no envio de mensagens por canais quânticos, apenas para citar alguns exemplos do potencial que pode ser extraído de estados emaranhados. Em particular, com base na medida de emaranhamento de Meyer e Wallach, e a sua descrição via códigos corretores de erros clássicos, é possível construir, de forma simples, estados quânticos emaranhados.

Por fim, na Seção 5.3, com base na codificação de rede proposta para a *rede borboleta*, propomos uma forma sistemática de como os nós intermediários de uma rede devem processar os pacotes de informações clássicas (subespaços vetoriais), descritos a partir de subestados de estados quânticos puros de máximo emaranhamento, e como os destinatários podem recuperar as informações transmitidas pela fonte.

As principais referências deste capítulo são (CUNHA, 2005; GAZZONI, 2008; NIELSEN, 2000).

5.1 Elementos de Mecânica Quântica

Nesta seção, descrevemos os conceitos básicos e fundamentais da mecânica quântica, necessários para o entendimento da nossa proposta de redes quânticas codificadas, que será explicitada no final deste capítulo. Tratam-se de conceitos de álgebra linear, descritos a partir da notação usual em mecânica quântica. Para uma revisão mais completa dos conceitos e resultados de álgebra linear e as suas aplicações na mecânica quântica, recomendamos (LANG, 2004; NIELSEN, 2000).

O postulado apresentado a seguir (NIELSEN, 2000) justifica o porquê da álgebra linear ser a linguagem necessária para uma descrição matemática da mecânica quântica.

Postulado: *Todo sistema físico isolado está associado a um espaço vetorial complexo com produto interno (Espaço de Hilbert), conhecido como o espaço de estados do sistema. O sistema é completamente descrito pelo seu vetor estado, o qual é um vetor unitário no espaço de estados do sistema.*

De posse deste postulado, seja $\mathbb{C}^m$ o espaço vetorial complexo de dimensão finita m, definido a partir das operações usuais, e que admite um produto interno. De agora em diante, faremos referência a este espaço vetorial euclidiano como um espaço de Hilbert. Assumindo a notação usual da mecânica quântica, isto é, a notação de Dirac, os vetores de $\mathbb{C}^m$, que também podem ser vistos como matrizes de ordem $m \times 1$, serão descritos como $|\psi\rangle$, onde $|.\rangle$ é dito *ket*. Assim, dada uma base $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_m\rangle\}$ de $\mathbb{C}^m$, o vetor $|\psi\rangle$ pode ser unicamente descrito como

$$|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle + \ldots + \alpha_m|\psi_m\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{pmatrix}. \tag{5.1}$$

Em particular, consideraremos como base do espaço de Hilbert $\mathbb{C}^m$ a base canônica, onde cada vetor que compõe esta base é composto por apenas uma coordenada não nula, que é dada pelo número complexo 1. É de verificação direta que tal base é ortonormal (LANG, 2004).

Exemplo 5.1.1. *Do ponto de vista da mecânica quântica, o vetor* $(\alpha_1, \alpha_2) \in \mathbb{C}^2$ *pode ser descrito como*

$$|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle, \tag{5.2}$$

onde $|\psi_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ *e* $|\psi_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Os vetores $|\psi_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e $|\psi_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ recebem uma notação especial, por conta do papel que desempenham no contexto quântico. Na verdade, tais vetores desempenham

o papel dos bits 0 e 1 nos sistemas digitais clássicos. Assim, devido a esta analogia, denotaremos $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Logo, reescrevendo o estado $|\psi\rangle$ (5.2) a partir destas notações, isto é,

$$|\psi\rangle = \alpha_1|0\rangle + \alpha_2|1\rangle, \tag{5.3}$$

denominaremos tal estado como um *qubit* ou bit quântico.

O vetor dual ao vetor $|\psi\rangle$ é denotado como $\langle\psi|$ e é lido como *bra*. Como $\mathbb{C}^m$ é um espaço de Hilbert, então o produto interno $\langle .,. \rangle$ entre os vetores $|\psi\rangle$ e $|\phi\rangle$ será descrito, novamente seguindo a notação usual da mecânica quântica, como

$$\begin{array}{rccc} \langle .,. \rangle : & \mathbb{C}^m \times \mathbb{C}^m & \to & \mathbb{C} \\ & (|\psi\rangle, |\phi\rangle) & \mapsto & \langle |\psi\rangle, |\phi\rangle \rangle = \langle \psi|\phi\rangle, \end{array} \tag{5.4}$$

e tal aplicação satisfaz as seguintes condições

(i) $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$, onde * é o complexo conjugado;

(ii) $\langle\psi|\left(a|\phi\rangle + b|\varphi\rangle\right)\rangle = a\langle\psi|\phi\rangle + b|\langle\psi|\varphi\rangle$;

(iii) $\langle\psi|\psi\rangle > 0$ se $|\psi\rangle \neq 0$,

para quaisquer vetores $|\psi\rangle, |\phi\rangle$ e $|\varphi\rangle \in \mathbb{C}^m$ e escalares $a, b \in \mathbb{C}$.

Considere $A : \mathbb{C}^m \to \mathbb{C}^m$ um operador linear, representado a partir da sua forma matricial. Assim, dado $|\psi\rangle \in \mathbb{C}^m$, como descrito em (5.1), temos

$$\begin{aligned} A\left(|\psi\rangle\right) &= A\left(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle + \ldots + \alpha_m|\psi_m\rangle\right) \\ &= \alpha_1 A\left(|\psi_1\rangle\right) + \alpha_2 A\left(|\psi_2\rangle\right) + \ldots + \alpha_m A\left(|\psi_m\rangle\right). \end{aligned} \tag{5.5}$$

A observação descrita em (5.5) é importante para este trabalho, pois ela representa, por exemplo, como um ruído quântico pode agir durante a transmissão de uma informação sobre um canal quântico. De forma muito breve, esta afirmação será revista na Subseção 5.2.1 e, para uma análise mais completa, recomendamos a leitura de (NIELSEN, 2000).

5.1.1 Produto Tensorial

Produto tensorial é um instrumento fundamental em mecânica quântica para a descrição de sistemas quânticos de multipartículas, isto é, sistemas quânticos formados a partir de outros sistemas menores. Tais sistemas multipartículas podem estar diretamente relacionados com o fenômeno físico conhecido como emaranhamento, que é objeto de estudo neste capítulo, e será descrito na próxima Seção 5.2. Assim, nesta subseção, faremos uma breve revisão sobre produto tensorial, de acordo com a necessidade deste texto.

Dados dois espaços vetoriais V e W de dimensão m e n, respectivamente, o espaço vetorial $V \otimes W$ possui dimensão mn e é gerado por combinações lineares finitas de vetores da forma $|\psi\rangle \otimes |\phi\rangle$, onde $|\psi\rangle \in V$ e $|\phi\rangle \in W$. Em algumas referências (ver (NIELSEN, 2000)), o produto tensorial $|\psi\rangle \otimes |\phi\rangle$ é abreviado como $|\psi\phi\rangle$, e adotaremos esta notação, que será amplamente usada nas próximas seções.

Utilizando a representação matricial devida aos kets (vetores), apresentamos a seguir uma forma concreta de como realizar o produto tensorial entre dois kets, conhecida como *produto de Kronecker*: Dadas as matrizes

$$A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & ... & a_{mn} \end{pmatrix} \in M_{m\times n}(\mathbb{C}) \text{ e } B = \begin{pmatrix} b_{11} & b_{12} & ... & b_{1q} \\ b_{21} & b_{22} & ... & b_{2q} \\ \vdots & \vdots & \vdots & \vdots \\ b_{p1} & b_{p2} & ... & b_{pq} \end{pmatrix} \in M_{p\times q}(\mathbb{C}), \tag{5.6}$$

o produto $A \otimes B$ é definido como

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & ... & a_{1n}B \\ a_{21}B & a_{22}B & ... & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & ... & a_{mn}B \end{pmatrix} \in M_{mp\times nq}(\mathbb{C}). \tag{5.7}$$

Exemplo 5.1.2. *Dadas as matrizes* $\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix} \in M_{2\times 1}(\mathbb{C})$*, então*

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 4 \\ 6 \end{pmatrix} \text{ e}$$

$$\begin{pmatrix} 2 \\ 3 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \\ 3 \\ 6 \end{pmatrix}, \tag{5.8}$$

ou seja, o produto tensorial não é comutativo.

Exemplo 5.1.3. *Conforme estabelecido anteriormente, os qubits* $|0\rangle$ *e* $|1\rangle$ *estão associados, por exemplo, às matrizes* $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ *e* $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$*, respectivamente. Assim, o estado* $|010\rangle =$

$|0\rangle \otimes |1\rangle \otimes |0\rangle$ *está associado à matriz*

$$|0\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{5.9}$$

Dados V e W espaços vetoriais, os elementos do espaço produto tensorial $V \otimes W$ satisfazem as seguintes propriedades

(i) Para $a \in \mathbb{C}$ e $|\psi\rangle \in V$ e $|\phi\rangle \in W$, então $a\left(|\psi\rangle \otimes |\phi\rangle\right) = (a|\psi\rangle) \otimes |\phi\rangle = |\psi\rangle \otimes (a|\phi\rangle)$;

(ii) Para $|\psi_1\rangle, |\phi_1\rangle \in V$ e $|\varphi_2\rangle \in W$, então $(|\psi_1\rangle + |\phi_1\rangle) \otimes |\varphi_2\rangle = (|\psi_1\rangle \otimes |\varphi_2\rangle) + (|\phi_1\rangle \otimes |\varphi_2\rangle)$;

(iii) Para $|\psi_1\rangle \in V$ e $|\phi_2\rangle, |\varphi_2\rangle \in W$, então $|\psi_1\rangle \otimes (|\phi_2\rangle + |\varphi_2\rangle) = (|\psi_1\rangle \otimes |\phi_2\rangle) + (|\psi_1\rangle \otimes |\varphi_2\rangle)$.

Exemplo 5.1.4. *O ket* $|\chi\rangle = \frac{1}{2}\left(|00\rangle + |10\rangle + |01\rangle + |11\rangle\right)$ *pode ser reescrito como*

$$|\chi\rangle = \frac{1}{2}\left(|00\rangle + |10\rangle + |01\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right). \tag{5.10}$$

Após estas considerações e definições, podemos descrever, matematicamente, o significado de um estado quântico puro, que será a matéria prima essencial para a nossa proposta de redes quânticas codificadas.

Definição 5.1.5. *Um estado puro arbitrário com n qubits* $|\psi\rangle_n$ *é representado como*

$$|\psi\rangle_n = \alpha_0|00...0\rangle + \alpha_1|10...0\rangle + ..\alpha_{2^n-2}|11...0\rangle + \alpha_{2^n-1}|11...1\rangle, \tag{5.11}$$

onde $\alpha_0, ..., \alpha_{2^n-1} \in \mathbb{C}$ *e* $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$.

Observação 5.1.6. *Cada um dos kets de* (5.11) *é composto por n qubits, e as sequências lá descritas representam todas as possíveis combinações binárias de comprimento n, totalizando* 2^n *kets. Ainda, as constantes complexas* $\alpha_0, \alpha_1, ..., \alpha_{2^n-1}$ *são ditas amplitudes, e representam uma distruibuição de probabilidade em relação aos vetores da base.*

5.2 Emaranhamentos Quânticos

Nesta seção, apresentaremos uma definição matemática do conceito de emaranhamento de um estado quântico puro. Apesar de não ser fácil, para dizer, possível, descrever

uma definição formal do conceito de emaranhamento, exibimos alguns comentários sobre a importância dos estudos deste fenômeno físico devido as suas aplicações em computação e teoria da informação quânticas. Apresentamos um critério de separabilidade, ou seja, um critério que diz se um estado é não emaranhável (ou separável) para um sistema de estados bipartites. Tal critério é conhecido como Decomposição de Schmidt. Referências para outros importantes critérios de separabilidade serão indicadas. Por fim, na Subseção 5.2.1, comentamos sobre a medida de emaranhamento de Meyer e Wallach, uma espécie de quantificador de emaranhamento de um dado estado quântico, e apresentamos uma releitura desta medida utilizando conceitos de teoria de codificação clássica.

Os resultados desta seção são extraídos de (BRUß, 2002; CUNHA, 2005; GAZZONI, 2008).

Explicitar uma definição formal do conceito físico conhecido como emaranhamento parece impossível de ser feito, devido às diferentes interpretações que podem ser dadas para tal fenômeno, que dependem do ambiente onde este conceito é estudado, além do que emaranhamento de um sistema quântico está diretamente relacionado com interações quânticas entre dois subsistemas. Para ilustrar o que acaba de ser dito, vale citar uma afirmação de (BRUß, 2002), onde o autor observa que

> "Nossa visão da natureza do emaranhamento pode continuar a ser modificada nos próximos anos".

O nome emaranhamento (*Entanglement*) foi dado por Erwin Schrödinger para o fenômeno físico, oriundo da mecânica quântica, que foi observado por Einstein, Podolski e Rose em 1935 (EINSTEIN B. PODOLSKY, 1935). Apesar de a mecânica quântica ter sido comprovada experimentalmente, desde 1935 até os dias de hoje, muito pouco se sabe sobre o emaranhamento.

Richard Feynman observou que parecia impossível simular estados quânticos utilizando computação clássica. Assim, dá-se início às pesquisas para o nascimento e desenvolvimento da computação quântica, que continuam até hoje e, a partir do conceito de emaranhamento, mostra-se que tal computação supera a clássica em diversos aspectos. Apenas como exemplo, o algoritmo de Shor (SHOR, 1997) consegue reduzir imensamente o número de cálculos necessários para fatorar um número inteiro como produto de números primos e, assim, coloca em risco toda a criptografia RSA, que é mundialmente utilizada para a proteção de informações bancárias. Ainda, podemos citar outras aplicações do emaranhamento quântico relacionadas à teoria da informação quântica como, por exemplo, o teletransporte quântico e a codificação superdensa. Uma boa leitura sobre estes tópicos, dados de forma resumida, e que apresenta as principais referências bibliográficas sobre estes assuntos, pode ser vista em (GAZZONI, 2008). Sobre o contexto

de transmissão de informação via canais quânticos, abordaremos mais sobre essa área de pesquisa na Subseção 5.2.1.

A seguir, apresentamos diferentes visões de grandes especialistas na área sobre como o conceito de emaranhamento pode ser interpretado. Vale destacar que tais descrições foram extraídas de (BRUß, 2002) e, assim lá é explicitado, tais afirmações não são citações. Mais ainda, lá constam todas as referências bibliográficas de onde tais afirmações foram extraídas

Sobre emaranhamentos quânticos ...

- *Einstein/Podolsky/Rosen*: Uma função onda emaranhada não descreve a realidade física de uma forma completa.
- *E. Schrödinger*: Para um estado emaranhado, "o melhor conhecimento possível do todo não incluí o melhor conhecimento das suas partes."
- *J. Bell*: ... uma correlação que é mais forte do que qualquer correlação clássica.
- *D. Mermin*: ... uma correlação que contradiz a teoria dos elementos da realidade.
- *A. Peres*: " ... um truque que mágicos quânticos usam para produzir fenômenos que não podem ser imitados por mágicos clássicos".
- *C. Bennett*: ... um recurso que permite teleportação quântica.
- *P. Shor*: ... uma estrutura global da função onda que permite algoritmos mais rápidos.
- *A. Ekert*: ... uma ferramenta para a comunicação segura.
- *Família Horodecki*: ... necessário para as primeiras aplicações de aplicações positivas em física.

Após esta breve introdução sobre o conceito e a importância do estudo de emaranhamentos quânticos, vamos definir tal conceito matematicamente.

Definição 5.2.1. *Um estado puro arbitrário com n qubits* $|\psi\rangle_n$ *representado por*

$$|\psi\rangle_n = \alpha_0|00...0\rangle + \alpha_1|10...0\rangle + ..\alpha_{2^n-2}|11...0\rangle + \alpha_{2^n-1}|11...1\rangle, \tag{5.12}$$

onde $\alpha_0, ..., \alpha_{2^n-1} \in \mathbb{C}$ *e* $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$ *é dito separável se puder ser escrito como*

$$|\psi\rangle_n = |\psi_1\rangle_1 \otimes |\psi_2\rangle_1 \otimes ... \otimes |\psi_n\rangle_1, \tag{5.13}$$

onde $|\psi_1\rangle_1, |\psi_2\rangle_1, ..., |\psi_n\rangle_1$ *são estados puros com* 1 *qubit.*

Qualquer estado quântico puro que não admita a decomposição igual àquela dada em (5.13) é dito *emaranhado.*

Exemplo 5.2.2. *Os estados de Bell*

$$\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) \;\; e \;\; \left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right), \tag{5.14}$$

são exemplos de estados emaranhados.

Exemplo 5.2.3. *O estado*

$$|\chi\rangle = \frac{1}{2}\left(|00\rangle + |10\rangle + |01\rangle + |11\rangle\right) \tag{5.15}$$

é separável, pois

$$|\chi\rangle = \frac{1}{2}\left(|00\rangle + |10\rangle + |01\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right). \tag{5.16}$$

Em geral, à medida que a dimensão do espaço de estados cresce, os estados separáveis tornam-se cada vez mais raros (CUNHA, 2005).

A medida que a quantidade de qubits em cada ket de um estado quântico puro cresce, torna-se muito mais difícil verificar se o estado quântico em questão é separável ou emaranhado. Assim, apresentaremos um dos critérios de separabilidade mais conhecidos para estados quânticos puros bipartites (ou biparticionados), isto é, quando cada estado quântico puro $|\psi\rangle$ de um sistema quântico pode ser descrito na forma $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$.

Teorema 5.2.4. *(PERES, 1995, Decomposição de Schmidt) Seja U um espaço de Hilbert, tal que $U = V \otimes W$, com $dim(W) = m$ e $dim(V) = n$, com $m \leq n$, sem perda de generalidade. Dado um vetor unitário (estado quântico) arbitrário $|\psi\rangle \in U$, existem bases ortonormais $\{|v_i\rangle\}$ de V e $\{|w_j\rangle\}$ de W, tais que*

$$|\psi\rangle = \sum_{k=1}^{m} \lambda_k |v_k\rangle \otimes |w_k\rangle, \tag{5.17}$$

onde $\lambda_k > 0$ e $\sum_{k=1}^{m} \lambda_k^2 = 1$.

Os números λ_k e os conjuntos $\{|v_i\rangle\}$ e $\{|w_j\rangle\}$ são ditos *números e bases de Schmidt*, respectivamente. De posse dos números de Schmidt, temos

Teorema 5.2.5. *(EKERT, 1995) Um estado puro é separável se, e somente se, o número de Schmidt associado à sua decomposição é 1.*

Outros critérios de separabilidade, como os critérios de Peres, da família Horodecki e Nielsen e Kempe podem ser encontrados em (BRUß, 2002; GAZZONI, 2008).

Um outro ponto de vista relacionado ao emaranhamento é, de alguma forma, tentar quantificá-lo. Existem diversas formas de como “medir"o emaranhamento de um estado quântico puro, onde tal grandeza pode ser vista como um recurso, e que a quantidade de emaranhamento está diretamente relacionada com o desempenho da atividade a ser executada. Dentre as diversas medidas de emaranhamento, como a medida de Von Neumann das matrizes reduzidas e emaranhamento de formação e concorrência, e outras que podem ser encontradas em (GAZZONI, 2008), para a proposta deste trabalho, focaremos na Medida de Meyer e Wallach (MEYER, 2002).

5.2.1 Medida de Emaranhamento de Meyer e Wallach

Conforme foi citado anteriormente, existem diversas formas de quantificar o emaranhamento de um estado quântico puro. O foco deste trabalho é a medida de Meyer e Wallach (MEYER, 2002), uma vez que, de acordo com os resultados de (GAZZONI, 2008), esta medida de emaranhamento pode ser reescrita utilizando conceitos da teoria de codificação clássica, e tais conceitos são fundamentais para a proposta deste trabalho, apresentada na última seção deste capítulo.

Os resultados desta seção são extraídos de (GAZZONI, 2008; MEYER, 2002; SCOTT, 2004).

Seja $\mathbf{x}$=$x_1x_2...x_n$ uma n-upla binária associada ao conteúdo de um ket do estado quântico puro $|\psi\rangle_n$, onde x_j, para $j = 1, 2, ..., n$, representa a j-ésima coordenada de $\mathbf{x}$. A função linear (5.18) dada abaixo desempenha um papel fundamental na descrição da medida de emaranhamento de um estado quântico proposta por Meyer e Wallach.

$$\begin{aligned} \iota_j(b) : \left(\mathbb{C}^2\right)^{\otimes n} &\rightarrow \left(\mathbb{C}^2\right)^{\otimes n-1} \\ \mathbf{x} &\mapsto \iota_j(b)(\mathbf{x}) = \delta_{bx_j}|x_1\rangle \otimes |x_2\rangle \otimes ... \otimes |x_{j-1}\rangle \otimes |x_{j+1}\rangle \otimes ... \otimes |x_n\rangle, \end{aligned} \tag{5.18}$$

onde $x_i \in \{0, 1\}$ e $b \in \{0, 1\}$.

Proposição 5.2.6. *(SCOTT, 2004) Dado um estado quântico puro arbitrário com n qubits $|\psi\rangle$, a medida de emaranhamento global de Meyer e Wallach é dada por*

$$Q\left(|\psi\rangle\right) = \frac{4}{n}\sum_{j=1}^{n} D\left(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle\right), \tag{5.19}$$

onde

$$D\left(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle\right) = \langle\psi|\iota_j(0), \iota_j(0)|\psi\rangle \langle\psi|\iota_j(1), \iota_j(1)|\psi\rangle - |\langle\psi|\iota_j(0), \iota_j(1)|\psi\rangle|^2, \tag{5.20}$$

para todo $j = 1, 2, ..., n$.

O operador Q é invariante sob transformações unitárias locais e tal que $0 \leq Q \leq 1$. Assim, $Q(|\psi\rangle) = 0$ se, e somente se, $|\psi\rangle$ é um estado separável, e $Q(|\psi\rangle) = 1$ se, e somente se, $|\psi\rangle$ é um estado puro de máximo emaranhamento global.

De acordo com a proposta de (GAZZONI, 2008), é possível reproduzir a Proposição 5.2.6 a partir da notação e termos usuais da teoria de códigos corretores de erros, uma vez que as sequências binárias que compõe os kets de um estado quântico puro podem ser lidas como palavras código de um código binário definido no espaço de Hamming $\mathbb{F}_2^n$. Denote A_ψ o conjunto de todas as sequências que compõe os kets do estado quântico $|\psi\rangle$. Logo, reescrevendo a Proposição 5.2.6 temos

Proposição 5.2.7. *(GAZZONI, 2008) Seja $|\psi\rangle$ um estado quântico puro com amplitudes iguais a $\frac{1}{\sqrt{M}}$ e tal que o conjunto A_ψ satisfaz $d > 1$. Nestas condições, a seguinte equivalência é estabelecida*

$$Q(|\psi\rangle) \equiv Q'(|\psi\rangle) = \frac{4}{n}\frac{1}{M^2}\sum_{j=1}^{n} z_j.\,(M - z_j)\,, \tag{5.21}$$

onde z_j representa o número de n-uplas de A_ψ que têm 0 na j-ésima posição, para todo $j = \{1, 2, ..., n\}$, M denota a cardinalidade de A_ψ e d denota a mínima distância de Hamming neste conjunto.

Observação 5.2.8. *Apesar da restrição de que as amplitudes de $|\psi\rangle_n$ devem ser todas iguais, a Proposição 5.2.7 apresenta uma forma muito mais simples e prática para o cálculo de $Q(|\psi\rangle)$, do que aquela dada pela Proposição 5.2.6.*

Ainda, com base na Proposição 5.2.6, Wanessa (GAZZONI, 2008) caracteriza quando um estado quântico puro $|\psi\rangle$ admite máximo emaranhamento.

Teorema 5.2.9. *(GAZZONI, 2008) Seja $|\psi\rangle$ um estado quântico puro com amplitudes iguais a $\frac{1}{\sqrt{M}}$, cujo conjunto A_ψ associado satisfaz $d > 1$ e tem cardinalidade M. Então, $|\psi\rangle$ é um estado quântico puro de máximo emaranhamento global se, e somente se, $z_j = \frac{M}{2}$, para todo $j \in \{1, 2, ..., n\}$.*

Conforme pode ser observado no Teorema 5.2.9, os códigos de bloco binários A_ψ que garantem o máximo emaranhamento global de $|\psi\rangle$ são os códigos de peso constante. Os códigos simplex lineares e não lineares, Nordstrom-Robinson e Preparata são exemplos de famílias de códigos de peso constante, cujas palavras código podem ser utilizadas como sequências dos kets de estados quânticos de máximo emaranhamento. Para maiores informações sobre essas famílias de códigos de peso constante, recomendamos a leitura de (MACWILLIAMS, 1983).

Observação 5.2.10. *De agora em diante, salvo menção ao contrário, seguindo o que é proposto pelo Teorema 5.2.9, apenas descreveremos estados quânticos puros $|\psi\rangle$, tais que $|A_\psi| = M$ e as respectivas amplitudes sejam $\frac{1}{\sqrt{M}}$.*

Na busca pelos melhores códigos de bloco binários que satisfaçam as condições do Teorema 5.2.9, conforme é constatado em (GAZZONI, 2008) a partir da análise dos parâmetros, isto é, uma grande cardinalidade de palavras código aliada a uma boa distância mínima, verificou-se que os códigos simplex lineares, que são códigos de peso constante, são bons candidatos para a tarefa de proteger as informações vinculadas a um estado quântico puro. Por definição, o código simplex é definido como sendo o código dual de um código de Hamming e, a partir desta definição, tal código possui 2^m palavras código de comprimento $2^m - 1$, onde o peso de cada palavra é igual a 2^{m-1}, o que implica que a distância mínima deste código é 2^{m-1}, para $m > 1$. A construção da matriz geradora do código simplex é bastante simples: Se desejamos obter um $(2^m - 1, 2^m, 2^{m-1})$ −código simplex, basta considerarmos todas as possíveis sequências binárias não nulas de comprimento m, e cada uma destas sequências será uma coluna da matriz geradora do código.

Durante todo este trabalho, apenas diremos códigos simplex em alusão aos códigos de bloco simplex lineares.

Exemplo 5.2.11. *Se desejamos obter um* $(3, 4, 2)-$*código simplex* $\mathcal{C}_2$*, verificamos que* $10, 01$*, e* 11 *são todas as sequências binárias não nulas de comprimento* $m = 2$*. Logo, a matriz geradora* H_2 *de* $\mathcal{C}_2$ *é*

$$H_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \Rightarrow \mathcal{C}_2 = \{000, 011, 101, 110\}. \tag{5.22}$$

Já para o caso em que $m = 3$*, logo as sequências binárias não nulas são* 100*,* 010*,* 001*,* 110*,* 101*,* 011*,* 111*, e dispondo-as como colunas de uma matriz, obtemos*

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \tag{5.23}$$

$$\Rightarrow \mathcal{C}_3 \{0000000, 0001111, 0110011, 1010101, 0111100, 1011010, 1100110, 1101001\}.$$

Observação 5.2.12. *As matrizes geradoras de códigos simplex podem ser vistas como submatrizes de um código de Reed-Muller. Esta e outras informações relativas a esta família de códigos de bloco podem ser encontradas em (MACWILLIAMS, 1983).*

Além da questão de garantir estados quânticos com máximo emaranhamento, outra vantagem de se utilizar palavras código de um código simplex como sequências de qubits do dado estado quântico, é a possibilidade de corrigir erros que por ventura venham ocorrer durante a transmissão deste estado, visto como uma informação. Neste caso, adentramos no campo de pesquisa da teoria da informação quântica e, em particular, na transmissão de informação via canais quânticos.

Na teoria da informação clássica, o canal que transmite uma informação (que, em geral, pode ser vista como uma sequência binária) de uma dada fonte está sujeito a diversas ações que, de alguma forma, podem alterar a informação que chega ao destinatário. Tal alteração é dada por um operador que troca o dígito 0 por 1, e vice-versa. Já no contexto da teoria da informação quântica, a informação pode ser descrita como uma sequência de qubits $|0\rangle$ e $|1\rangle$, e há uma gama maior de ações do canal quântico que podem alterar a informação que chega ao destinatário. Os operadores quânticos que agem sob um canal quântico durante a transmissão são descritos como combinações das seguintes matrizes

$$
\begin{array}{rcrcl}
I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \Rightarrow & I|0\rangle & = & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle; \\
 & \Rightarrow & I|1\rangle & = & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle; \\
X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \Rightarrow & X|0\rangle & = & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle; \\
 & \Rightarrow & X|1\rangle & = & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |0\rangle; \\
Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & \Rightarrow & Z|0\rangle & = & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle; \\
 & \Rightarrow & Z|1\rangle & = & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle; \\
Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & \Rightarrow & Y|0\rangle & = & \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ -i \end{pmatrix} = -i|1\rangle; \\
 & \Rightarrow & Y|1\rangle & = & \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -i \\ 0 \end{pmatrix} = -i|0\rangle.
\end{array}
$$

Vale destacar que o operador X é o análogo do operador que age em um canal clássico durante a transmissão de informação.

Os operadores de erro $\{I, X, Y, Z\}$ admitem uma estrutura algébrica, a saber, a estrutura de grupo, e tal conjunto é conhecido com *grupo de Pauli*. De acordo com (NIELSEN, 2000), o efeito de um sistema temporal sobre um estado quântico é regido por operadores unitários, e que tais operadores unitários são gerados a partir do grupo de Pauli, assim justificando a importância deste grupo no contexto quântico e, em particular, para a teoria da informação quântica. Para mais informações sobre tais grupos, indicamos (NIELSEN, 2000; WEYL, 1950).

Voltando a questão do emprego de códigos corretores de erros clássicos no contexto da teoria da informação quântica, as palavras código de um código simplex, quando usadas como rótulos para os kets de um estado quântico puro $|\psi\rangle$, além de garantirem estados de máximo emaranhamento global (Vide Teorema 5.2.9), são bons códigos para a deteção e

correção de erros que possam vir a surgir, por exemplo, durante uma transmissão via um canal quântico.

Considere, por exemplo, que o seguinte estado quântico puro

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{8}}|0000000\rangle + \frac{1}{\sqrt{8}}|0001111\rangle + \frac{1}{\sqrt{8}}|0110011\rangle + \frac{1}{\sqrt{8}}|1010101\rangle + \frac{1}{\sqrt{8}}|0111100\rangle \\ &+ \frac{1}{\sqrt{8}}|1011010\rangle + \frac{1}{\sqrt{8}}|1100110\rangle + \frac{1}{\sqrt{8}}|1101001\rangle \end{aligned} \tag{5.24}$$

seja transmitido através de um canal quântico. Se, por alguma ação do canal quântico, o receptor receba o estado quântico puro

$$\begin{aligned} |\phi\rangle &= \frac{1}{\sqrt{8}}|1000000\rangle + \frac{1}{\sqrt{8}}|1001111\rangle + \frac{1}{\sqrt{8}}|1110011\rangle + \frac{1}{\sqrt{8}}|0010101\rangle + \frac{1}{\sqrt{8}}|1111100\rangle \\ &+ \frac{1}{\sqrt{8}}|0011010\rangle + \frac{1}{\sqrt{8}}|0100110\rangle + \frac{1}{\sqrt{8}}|0101001\rangle, \end{aligned} \tag{5.25}$$

onde $|\psi\rangle \neq |\phi\rangle$ (todas as primeiras coordenadas das sequências binárias foram alteradas) e, logo, observa-se que a informação transmitida pelo estado quântico puro $|\psi\rangle$ foi afetada por um ruído vindo do canal. Como o código que rotula os kets de $|\psi\rangle$ é um (7,8,4)-código simplex, logo tal código é habilitado a detetar um erro e corrigi-lo. Na verdade, esse código pode detetar todos os padrões de um erro, alguns de dois erros, e um caso de três erros. Assim, é possível que o receptor recupere a mensagem original $|\psi\rangle$ transmitida pela fonte.

5.3 Redes Quânticas

Em analogia ao problema abordado em (AHLSWEDE N. CAI, 2000) e de posse dos resultados dados na Seção 5.2, propomos uma construção teórica de uma rede capaz de processar e transmitir informações quânticas, que por sua vez, carregam pacotes de informações clássicas descritos a partir de subespaços vetoriais de $\mathcal{P}_q(n)$. Descrevemos uma forma de como relacionar um subespaço vetorial a cada ket de um estado quântico puro de máximo emaranhamento global (por meio da medida de Meyer e Wallach) utilizando conceitos básicos da teoria clássica de codificação e, a partir de uma aplicação definida entre pares de subespaços vetoriais, relacionamos aos novos subespaços vetoriais os respectivos subestados quânticos associados, obtidos como combinações dos kets do estado quântico puro dado. Um exemplo de tal rede é dado, sendo um análogo da rede borboleta, amplamente estudada entre os pesquisadores da área de codificação de redes clássicas, isto é, redes que transmitem informações não-quânticas.

Vamos começar descrevendo a aplicação definida entre subespaços vetoriais.

Dados $V_1, V_2 \in \mathcal{P}_q(n)$, defina a seguinte aplicação, conhecida como *diferença simétrica*

$$V_1 \boxplus V_2 = \langle (V_1 \setminus V_2) \cup (V_2 \setminus V_1) \rangle \tag{5.26}$$

onde, por abuso de notação, $\langle A \rangle$ descreve o subespaço vetorial de $\mathbb{F}_q^n$ gerado pelo conjunto A. A aplicação $\boxplus$ satisfaz as seguintes condições

(i) $V \boxplus \{0\} = V$, para todo $V \in \mathbb{F}_q^n$;

(ii) $V \boxplus V = \{0\}$, para todo $V \in \mathbb{F}_q^n$;

(iii) $d_S(V_1, V_2) = d_S(V_1 \boxplus V_3, V_2 \boxplus V_3)$,

(iv) $(V_1 \boxplus V_2) \boxplus V_3 = V_1 \boxplus (V_2 \boxplus V_3)$, para quaisquer $V_1, V_2, V_3 \in \mathcal{P}_q(n)$.

A aplicação $\boxplus$ (5.26) é constantemente usada como a operação definidora de códigos de subespaço lineares, que admitem a estrutura de grupo. A validade das propriedades $(i), (ii), (iii), (iv)$, bem como a definição de códigos de subespaço lineares, podem ser encontradas nas referências (BRAUN T. ETZION, 2013; PAI, 2015).

Nesta seção, propomos uma hipotética rede *multicast* de transmissão de informações quânticas, com base nas contribuições de (AHLSWEDE N. CAI, 2000; KöTTER, 2008), e as referências lá contidas, bem como nos resultados oriundos da teoria de codificação clássica (MACWILLIAMS, 1983; UNGERBOECK, 1982). Basicamente, pretendemos transmitir diversas informações, descritas como vetores de $\mathbb{F}_q^n$, que podem ser vistas como o subespaço vetorial gerado por tais vetores. A este subespaço vetorial, associamos um subestado de um estado quântico puro $|\psi\rangle$ de máximo emaranhamento global.

A rede de transmissão de informações quânticas (RIQ) é apta a desenvolver as mesmas ações que uma rede clássica com codificação, isto é, dada uma rede RIQ, os nós intermediários desta rede são capazes de rotear as informações quânticas/subestados quânticos recebidas, bem como combinar uma quantidade finita destes subestados quânticos em um novo subestado quântico, que será encaminhado para os próximos nós da rede. Já foi visto na introdução deste trabalho, que redes, cujos nós intermediários são capazes de processar pacotes de informações, conseguem aumentar a taxa de transferência de informação por unidade de tempo quando comparadas a redes que não admitem codificação.

Considere, por exemplo, o estado quântico puro de máximo emaranhamento

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{8}}|0000000\rangle + \frac{1}{\sqrt{8}}|0001111\rangle + \frac{1}{\sqrt{8}}|0110011\rangle + \frac{1}{\sqrt{8}}|1010101\rangle + \frac{1}{\sqrt{8}}|0111100\rangle \\ &+ \frac{1}{\sqrt{8}}|1011010\rangle + \frac{1}{\sqrt{8}}|1100110\rangle + \frac{1}{\sqrt{8}}|1101001\rangle, \end{aligned} \tag{5.27}$$

onde denotaremos os subestados quânticos $|0000000\rangle$, $|0001111\rangle$ e $|0110011\rangle$ como $|\psi_1\rangle$, $|\psi_2\rangle$ e $|\psi_3\rangle$, respectivamente. Logo, a Figura 11 reproduz a proposta apresentada neste parágrafo.

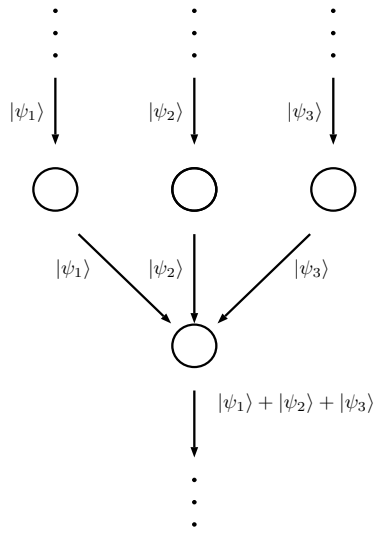


Figura 11 – Exemplo de uma rede RIQ processando três subestados quânticos

Agora, surgem os seguintes questionamentos: Dado um estado quântico puro de máximo emaranhamento $|\psi\rangle$ e os seus respectivos subestados, como faremos o processamento, por exemplo, de um par de subestados quânticos para obtermos um terceiro subestado quântico puro de $|\psi\rangle$? Ou, dado este terceiro subestado quântico puro, como recuperaremos os dois subestados quânticos originários? Antes de respondermos estas perguntas, vamos apresentar a forma com que desejamos associar os subespaços vetoriais aos subestados quânticos de $|\psi\rangle$.

Considere o estado quântico puro

$$|\psi\rangle_n = \alpha_0|00...0\rangle + \alpha_2|10...0\rangle + ... + \alpha_{2^n-2}|11...0\rangle + \alpha_{2^n-1}|11...1\rangle, \tag{5.28}$$

onde $\alpha_i \in \mathbb{C}$, $i = 0, 1, ..., 2^n - 1$, e $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$.

Vale destacar que para cada ket em (5.28) há um vetor associado com entradas complexas de comprimento 2^n. Esta associação é feita da seguinte forma: A sequência binária em cada ket descreve a representação binária de um número inteiro $0 \leq m < 2^n$. A este número m, associamos o vetor binário complexo formado por 0 em todas as posições, exceto na $(m+1)-$ésima entrada. Assim todo ket de (5.28) está associado a um elemento da base canônica (ortonormal) de $\mathbb{C}^{2^n}$.

Dados os resultados e notações de (GAZZONI, 2008) expressos na Subseção 5.2.1, devemos considerar estados quânticos puros $|\psi\rangle$, cujos respectivos elementos do conjunto A_ψ descrevem as palavras código de um código simplex (linear) tradicional. Como os parâmetros de um código simplex são da forma $(2^n - 1, 2^n, 2^{n-1})$, logo necessitamos de um código de subespaço $C \subset \mathcal{P}_q(n)$, tal que $|C| = 2^n$, pois cada subespaço será rotulado de acordo com a representação binária de um inteiro m, tal que $0 \leq m < 2^n$ e, posteriormente, será rotulado como uma palavra código de um código simplex. Para o rotulamento a partir

da representação binária de inteiros, usaremos o Particionamento de Conjuntos proposto na Subseção 4.2.1. Tal rotulamento é vantajoso, uma vez que oferece uma forma padrão de distribuir os rótulos entre os subespaços, além de abrir a oportunidade para diversas outras formas de rotulamento para as palavras código de um código de subespaço, por exemplo, a partir de códigos concatenados e códigos de treliça.

A seguir, apresentamos um exemplo que ilustra as considerações dadas no parágrafo anterior sobre as duas formas de rotulamento propostas.

Exemplo 5.3.1. *Dados que* $p(x) = x^6 + x + 1 \in \mathbb{F}_2[x]$ *é um polinômio primitivo e* $\alpha \in \mathbb{F}_{2^6}$ *é uma de suas raízes, onde* $\mathbb{F}_{2^6} \simeq \mathbb{F}_2[x]/\langle p(x)\rangle$*, considere o código de subespaço* $C = \{V_1, V_2, V_3, V_4\} \subset \mathcal{G}_2(6,2)$*, tal que* $V_1 = \{0, 1, \alpha, \alpha^6\}$*,* $V_2 = \{0, \alpha, \alpha^2, \alpha^7\} = \alpha V$*,* $V_3 = \{0, \alpha^2, \alpha^3, \alpha^8\} = \alpha^2 V$ *e* $V_4 = \{0, \alpha^3, \alpha^4, \alpha^9\} = \alpha^3 V$*. Particione o código* C*, por exemplo, como* $C = C_1 \cup C_2$*, onde* $C_1 = \{V_1, V_2\}$ *e* $C_2 = \{V_3, V_4\}$*. As palavras código de* C *serão rotuladas de acordo com os caminhos e os respectivos rótulos dados pela Figura 12, onde "*$i, \delta_i = j$*"denota que, no nível* i*, a menor distância de subespaço* (δ_i) *dentre todos os conjuntos daquele nível é* j*. Além disso, utilizamos o símbolo* ∞ *para descrever a distância mínima nos conjuntos unitários.*

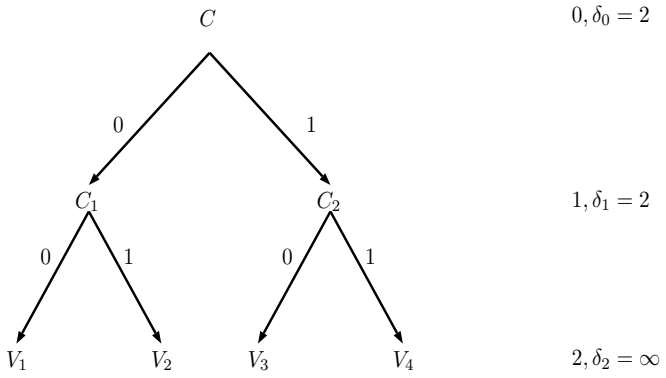


Figura 12 – Particionamento de Conjunto do código $C = \{V_1, V_2, V_3, V_4\}$

Os rotulamentos propostos pela Figura 12 são $V_1 = (00)$*,* $V_2 = (01)$*,* $V_3 = (10)$ *e* $V_4 = (11)$*, e também podem ser vistos como a representação binária dos números inteiros de* 0 *a* 3*.*

Em conformidade com a proposta de (GAZZONI, 2008), para obtermos estados quânticos de máximo emaranhamento via a medida de Meyer e Wallach, as sequências binárias que compõe os kets de um estado quântico puro devem ser associadas às palavras código de um código simplex clássico. Portanto, os rótulos dados pela Figura 12 serão associados às palavras código de um $(3,4,2)-$*código simplex da seguinte forma: Como a matriz geradora do* $(3,4,2)-$*código simplex é* $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$*, então os subespaços de* C*, na*

verdade, serão rotulados como

$$(00).\begin{pmatrix}0&1&1\\1&0&1\end{pmatrix}=(000),\ (01).\begin{pmatrix}0&1&1\\1&0&1\end{pmatrix}=(101),\ (10).\begin{pmatrix}0&1&1\\1&0&1\end{pmatrix}=(011)\ e$$
$$(11).\begin{pmatrix}0&1&1\\1&0&1\end{pmatrix}=(110). \tag{5.29}$$

Subespaço vetorial	Particionamento de Conjuntos, nº inteiro	Código simplex
V_1	(00),0	(000)
V_2	(01),2	(101)
V_3	(10),1	(011)
V_4	(11),3	(110)

Tabela 5 – Diferentes representações para os subespaços de C

Assim, os subespaços V_1, V_2, V_3 e V_4 são associados aos subestados quânticos/kets $|000\rangle$, $|101\rangle$, $|011\rangle$ e $|110\rangle$, respectivamente, do estado quântico puro de máximo emaranhamento

$$|\psi\rangle=\frac{1}{2}|000\rangle+\frac{1}{2}|101\rangle+\frac{1}{2}|011\rangle+\frac{1}{2}|110\rangle. \tag{5.30}$$

O estado quântico puro $|\psi\rangle$ possui um total de $2^4=16$ subestados quânticos. Tal quantidade é obtida a partir do conjunto das partes de $\{|000\rangle,|101\rangle,|011\rangle,|110\rangle\}$. Cada subestado quântico puro de $|\psi\rangle$ está associado a um subespaço vetorial de $\mathbb{F}_{2^6}$, gerado pela operação (5.26) *e os elementos de C. Todos os subespaços vetoriais e os respectivos subestados quânticos de $|\psi\rangle$ são descritos na Tabela* 6*, e vale destacar que para este caso, a operação $\boxplus$ está bem definida.*

Salientamos que o (3,4,2)-código simplex utilizado para rotular os kets do estado quântico puro (5.30) *apenas deteta erro e não oferece proteção a erros.*

Observação 5.3.2. *A escolha dos subespaços que compõe o código C deve ser feita observando o fato de que, para a operação $\boxplus$ ser bem definida, a dimensão dos elementos de C deve ser baixa em relação a dimensão de $\mathbb{F}_q^n$ pois, do contrário, pode ocorrer que $X\boxplus Y=X\boxplus Z$, para palavras código distintas $X,Y,Z\in C$.*

Seja C um código de subespaço associado aos subestados quânticos de um estado quântico puro emaranhado $|\psi\rangle$, seguindo o procedimento explicitado no Exemplo 5.3.1. Respondendo aos questionamentos feitos anteriormente, precisamos explicitar como os nós intermediários das redes quânticas processam os subestados quânticos recebidos, e como esse processamento afeta os subespaços representados por tais subestados. Além disso, dado o processamento de um par de subestados quânticos de $|\psi\rangle$, devemos definir uma forma de como recuperar estes dois subestados. As respostas para tais questionamentos serão dadas a partir do seguinte procedimento: Dado que os subestados quânticos $|\psi_1\rangle$ e

Subespaço vetorial	Subestado quântico
$V_1 = \langle 1, \alpha \rangle$	$\|000\rangle$
$V_2 = \langle \alpha, \alpha^2 \rangle$	$\|101\rangle$
$V_3 = \langle \alpha^2, \alpha^3 \rangle$	$\|011\rangle$
$V_4 = \langle \alpha^3, \alpha^4 \rangle$	$\|110\rangle$
$V_1 \boxplus V_2 = \langle 1, \alpha^2, \alpha^6 \rangle$	$\|000\rangle + \|101\rangle$
$V_1 \boxplus V_3 = \langle 1, \alpha, \alpha^2, \alpha^3 \rangle$	$\|000\rangle + \|011\rangle$
$V_1 \boxplus V_4 = \langle 1, \alpha, \alpha^3, \alpha^4 \rangle$	$\|000\rangle + \|110\rangle$
$V_2 \boxplus V_3 = \langle \alpha, \alpha^3, \alpha^7, \alpha^8 \rangle$	$\|101\rangle + \|011\rangle$
$V_2 \boxplus V_4 = \langle \alpha, \alpha^2, \alpha^3, \alpha^4 \rangle$	$\|101\rangle + \|110\rangle$
$V_3 \boxplus V_4 = \langle \alpha^2, \alpha^4, \alpha^8, \alpha^9 \rangle$	$\|011\rangle + \|110\rangle$
$V_1 \boxplus V_2 \boxplus V_3 = \langle 1, \alpha^3, \alpha^6, \alpha^8 \rangle$	$\|000\rangle + \|101\rangle + \|011\rangle$
$V_2 \boxplus V_3 \boxplus V_4 = \langle \alpha, \alpha^4, \alpha^7, \alpha^8, \alpha^9 \rangle$	$\|000\rangle + \|101\rangle + \|011\rangle$
$V_1 \boxplus V_2 \boxplus V_4 = \langle 1, \alpha^2, \alpha^3, \alpha^4, \alpha^6 \rangle$	$\|000\rangle + \|101\rangle + \|110\rangle$
$V_1 \boxplus V_3 \boxplus V_4 = \langle 1, \alpha, \alpha^2, \alpha^4, \alpha^9 \rangle$	$\|000\rangle + \|011\rangle + \|110\rangle$
$V_1 \boxplus V_2 \boxplus V_3 \boxplus V_4 = \langle 1, \alpha^4, \alpha^6, \alpha^8, \alpha^9 \rangle$	$\|000\rangle + \|101\rangle + \|011\rangle + \|110\rangle$

Tabela 6 – Subespaços vetoriais e os respectivos subestados quânticos de $|\psi\rangle$ associados

$|\psi_2\rangle$ de $|\psi\rangle$ estão associados aos subespaços V_1 e V_2, respectivamente, então o subestado quântico $|\psi_1\rangle + |\psi_2\rangle$ está associado ao subespaço

$$V_1 \boxplus V_2 = |\psi_1\rangle + |\psi_2\rangle, \tag{5.31}$$

isto é, as operações realizadas nos nós intermediários de uma possível rede quântica serão baseadas na operação $\boxplus$ (5.26), definida entre os subespaços vetoriais associados. Vale destacar que consideraremos que os subestados quânticos sempre possuem amplitudes iguais, e omitiremos tais valores.

Considere uma hipotética rede "borboleta"quântica, descrita pela Figura 13, onde existem uma fonte (F) e dois destinatários (D_1 e D_2). Assim como no caso das redes lineares clássicas com codificação, os nós intermediários são capazes de rotear as informações, bem como processá-las em uma nova informação e encaminhá-la para o próximo nó, o que garante um ganho na taxa de transferência de informação com relação às redes que não admitem codificação.

Suponha que a fonte F envie dois subestados quânticos $|\psi_1\rangle$ e $|\psi_2\rangle$ distintos, que estão associados aos subespaços vetoriais distintos $V_1, V_2 \in \mathcal{P}_q(n)$, respectivamente, onde $|\psi_1\rangle$ segue em direção ao nó 1 e $|\psi_2\rangle$ segue em direção ao nó 2. Estes subestados quânticos serão encaminhados para o nó 3 e para os destinatários D_1 e D_2, conforme ilustrado na Figura 13. Como o nó 3 é capaz de processar tais informações, a nova informação $|\psi_1\rangle + |\psi_2\rangle$, que corresponde ao subespaço vetorial $V_1 \boxplus V_2$, será encaminhada ao nó 4, que por sua vez encaminhará para os nós destinatários D_1 e D_2.

Como a aplicação $\boxplus$ é associativa, comutativa e $V \boxplus V = \{0\}$, então os destinatários

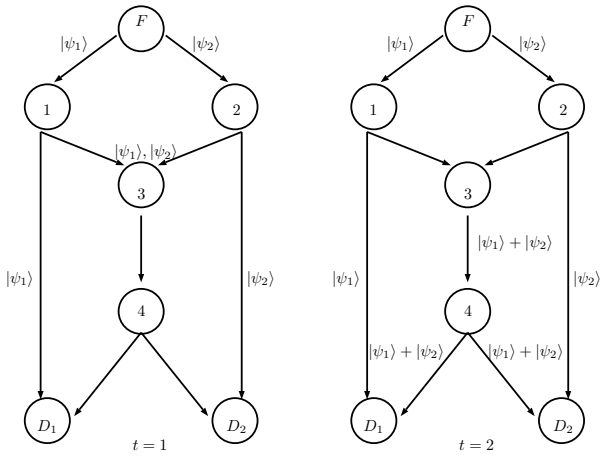


Figura 13 – Rede borboleta quântica

D_1 e D_2 executam as seguintes operações sobre as informações recebidas

$$\begin{aligned} \text{Em } D_1: \quad (V_1 \boxplus V_2) \boxplus V_1 &= V_2 \boxplus (V_1 \boxplus V_1) = V_2 \mapsto |\psi_2\rangle \text{ e} \\ \text{Em } D_2: \quad (V_1 \boxplus V_2) \boxplus V_2 &= V_1 \boxplus (V_2 \boxplus V_2) = V_1 \mapsto |\psi_1\rangle. \end{aligned} \tag{5.32}$$

Assim, os destinatários D_1 e D_2 conseguem recuperar as informações $|\psi_2\rangle$ e $|\psi_1\rangle$, respectivamente e, portanto, as mensagens $|\psi_1\rangle$ e $|\psi_2\rangle$ são entregues aos destinatários, exatamente como ocorre com uma rede borboleta clássica que admite codificação.

5.4 Comentários Finais

Neste capítulo, propusemos uma situação teórica em que uma rede linear é apta a transmitir informações quânticas. Não há nenhuma evidência de que seja possível reproduzir tal rede para fins práticos, mas o objetivo central aqui é aliar duas importantes áreas do conhecimento que, a princípio, pareciam disjuntas.

Iniciamos este capítulo com uma breve revisão sobre alguns conceitos básicos de mecânica quântica, definidos com base em um postulado que relaciona espaços de estados quânticos com espaços vetoriais complexos. Dada esta fundamentação matemática, apresentamos as definições de qubit, que desenvolve um papel análogo ao do bit na teoria da informação quântica, e estados quânticos puros. A composição de qubits em busca de sequências maiores é feita com base na operação produto tensorial, logo se faz necessária uma rápida revisão sobre esta operação.

Em seguida, abordamos um tópico que merece destaque, tanto pelas suas diversas aplicações em computação e teoria da informação quântica, quanto pelo desconhecimento que existe em torno do seu completo entendimento. Trata-se do conceito de emaranhamento quântico. Dentre os diversos critérios de separabilidade e medidas de emaranha-

mento existentes na literatura, focamos em uma releitura da medida de emaranhamento de Meyer e Wallach, conectando-a com a teoria de codificação clássica.

Dadas as condições necessárias e suficientes para a descrição de estados quânticos puros emaranhados, é proposto uma forma de associar subespaços vetoriais aos kets de um dado estado quântico puro emaranhado. A princípio, cada um dos subespaços vetoriais é associado a representação binária de um inteiro, que por sua vez é associada a uma palavra código de um código simplex linear tradicional. Tais palavras código, que também são sequências binárias, descrevem as sequências de qubits associadas ao kets de um estado quântico emaranhado. Tal sistematização se mostra importante para a proteção das informações vinculadas, além de estruturar possíveis procedimentos de decodificação. A viabilidade deste procedimento, por exemplo, a partir da análise do custo operacional deste processo, fica como um tópico de pesquisa futura.

Por fim, de posse da forma sistemática de associação entre subespaços vetoriais e kets de um estado quântico puro emaranhado, descrevemos uma forma de como os nós de uma possível rede linear de transmissão de informações quânticas devem processar as informações recebidas. Este procedimento deve respeitar os subespaços e os respectivos kets associados, agindo como um operador lógico *xor*. Como um exemplo, descrevemos uma hipotética rede borboleta transmissora de informações quânticas e detalhamos como os nós destinatários podem recuperar as informações inicialmente transmitidas pela fonte.

Conclusões e Sugestões para Trabalhos Futuros

Neste trabalho, inicialmente, propomos uma investigação sobre códigos geometricamente uniformes em $\mathcal{G}_q(n,k)$. Verificou-se que tais códigos podem ser descritos a partir dos códigos de órbita. Logo, dada a uniformidade geométrica dos códigos de órbita, apresentamos uma releitura de conceitos clássicos aplicados ao contexto de codificação de redes, permitindo-nos melhor compreender as estruturas algébrica e geométrica destes códigos, e quais vantagens podem ser extraídas dessas estruturas em relação aos problemas oriundos da teoria da informação de redes.

Em um segundo momento, descrevemos uma proposta teórica e inicial de como uma rede linear quântica pode ser desenvolvida, de forma que, associando subespaços vetoriais aos subestados quânticos de um estado quântico puro emaranhado, possamos processar esses subestados quânticos e, consequentemente, os subespaços vetoriais associados.

Em relação aos trabalhos anteriores sobre códigos de órbita, nenhum destes abordou o ponto de vista de tais códigos como sendo geometricamente uniformes. Ainda, sobre códigos de órbita gerados por grupos abelianos, além do caso cíclico, não foram observados resultados ou quaisquer referências a essa classe mais geral de códigos no contexto de codificação de redes. Sobre a proposta de construção de redes lineares quânticas, até o presente momento, não havia referência na literatura sobre esse estudo.

A releitura de conceitos clássicos se mostrou útil, por exemplo, a partir do momento em que consideramos o estudo das partições geometricamente uniformes de um código de órbita abeliano, de onde pudemos extrair um resultado que reduz consideravelmente o número de operações necessárias para a obtenção da distância de subespaço mínima do código. Também, de posse do conceito de regiões de Voronoi, exibimos um procedimento de decodificação bastante simples.

Outro ponto contido no Capítulo 4 que merece destaque é a construção de cadeias de partições geometricamente uniformes e a construção multinível associada onde, de posse de um resultado clássico de códigos geometricamente uniformes, foi possível construir um código L-nível e, novamente, reduzir o número de operações necessárias para descrever a distância mínima deste código multinível.

No Capítulo 5, propusemos, ainda que inicialmente, uma conexão entre os códigos de subespaço com a teoria da informação quântica, que é um objeto atual de pesquisa devido às excelentes expectativas de potenciais aplicações práticas, caso tal proposta seja

implementável. Dados os diversos benefícios já vistos no emprego de estados quânticos emaranhados nos mais diversos contextos quânticos ligados a transmissão de informação, buscamos agora não associarmos apenas palavras código aos kets de um estado quântico, mas sim associarmos subespaços vetoriais, ou seja, conectar a teoria que Köetter e Kschischang propuseram para redes lineares aleatórias com o que há de mais praticado em teoria da informação quântica, isto é, de forma bastante grosseira, buscamos considerar uma rede capaz de transmitir e processar informações quânticas.

Sugestões para Futuras Pesquisas

Como uma sequência deste trabalho, propomos os seguintes tópicos de investigação:

(i) Tentar obter uma fórmula que descreva a distribuição de pesos de um código de órbita abeliano $C_G(V)$. Para esta situação, dado um subgrupo $H \lhd G$, parece razoável analisar uma partição geometricamente uniforme deste código e os respectivos polinômios $F\left(w, g_j, C_H\left(Vg_i\right)\right)$, para $g_i, g_j \in G/H$ e $g_i \neq g_j$.

(ii) Calcular a complexidade do algoritmo de decodificação para códigos de órbita tendo como base as regiões de Voronoi. Este custo é menor que o custo operacional do algoritmo de decodificação baseado em síndromes proposto por (TRAUTMANN F. MANGANIELLO, 2013)?

(iii) Aplicar códigos de órbita, ou seja, códigos geometricamente uniformes, no contexto descrito no Capítulo 5. Em geral, dar sequência ao estudo e desenvolvimento da teoria de redes de transmissão de informações quântica.

Comentários Finais

O estudo de códigos de subespaço e, em particular, de códigos de órbita, é bastante recente e promissor, devido à estrutura algébrica que dá sustentação à geração destes códigos. Dada a caracterização direta desses códigos como códigos geometricamente uniformes, podemos também fazer uso de uma rica estrutura geométrica e, assim, aliando tais estruturas, direcionar as pesquisas em prol do avanço na busca por códigos com melhores parâmetros e/ou na busca de bons algoritmos de decodificação.

Por outro lado, a aplicação de conceitos de física quântica em procedimentos de transmissão de informação também é bastante recente e promissora, dados os resultados iniciais já vistos na literatura e as conjecturas sobre possíveis aplicações práticas. Assim, no final deste trabalho, levantamos o questionamento de porque não aliarmos estas duas

recentes áreas de estudo, na busca de novas ideias que possam, futuramente, serem aplicadas a situações do nosso cotidiano, com ganhos em segurança, velocidade, dentre outros pontos.

Esperamos que este trabalho incentive novos e experientes pesquisadores a obterem novas informações sobre códigos de órbita, na busca por melhores códigos, além de outras interseções entre os códigos de subespaço e a teoria da informação quântica.

Referências

AHLSWEDE N. CAI, R. L. R. W. Y. R. Network Information Flow. *IEEE Transactions On Information Theory*, v. 46, p. 1204–1216, 2000.

BAER, R. *Linear Algebra and Projective Geometry*. 3. ed. [S.l.]: Academic Press, 1952.

BARDESTANI, A. I. F. Cyclic Orbit Codes with the Normalizer of a Singer Subgroup. *Journal of Sciences, Islamic Republic of Iran*, v. 26, p. 49–55, 2015.

BIGLIERI, M. E. E. Multidimensional Modulation and Coding for Band-Limited Digital Channels. *IEEE Transactions on Information Theory*, v. 34, p. 803–809, 1988.

BLAKE, R. M. I. *The Mathematical Theory of Coding*. [S.l.]: Academic Press, 1975.

BRAUN T. ETZION, A. V. M. Linearity and Complements in Projective Space. *Linear Algebra and Its Applications*, v. 438, p. 57–70, 2013.

BRUß, D. Characterizing entanglement. *Journal of Mathematical Physics*, v. 43, p. 4237–4251, 2002.

CALDERBANK, A. R. Multilevel Codes and Multistage Decoding. *IEEE Transactions on Communications*, v. 37, p. 222–229, 1989.

CONWAY, N. S. J. *Sphere Packings, Lattices and Groups*. [S.l.]: Springer-Verlag, 1999.

CUNHA, M. de O. T. *Emaranhamento: Caracterização, Manipulação e Consequências*. [S.l.]: Tese de doutoramento, UFMG, Belo Horizonte, MG, 2005.

DARAFSHEH, M. Order of Elements in the Groups Related to the General Linear Group. *Finite Fields and Their Applications*, v. 11, p. 738–747, 2005.

DYE, R. H. Maximal Subgroups of Sympletic Groups Stabilizing Spreads II. *Journal of the London Mathematical Society*, v. 40, p. 215–226, 1989.

EINSTEIN B. PODOLSKY, N. R. A. Can Quantum-Mechanical Description of Physical Reality be Considered Complete? *Physical Review Letters*, v. 47, p. 777, 1935.

EKERT, P. L. K. A. Entangled Quantum Systems and the Schmidt Decomposition. *American Journal of Physics*, v. 63, p. 415, 1995.

ETZION, A. V. T. Error-Correcting Codes in Projective Space. *IEEE Transactions on Information Theory*, v. 57, p. 1165–1173, 2011.

ETZION, T. Problems on q-Analogs in Coding Theory. *Preprint arXiv:13056126 [cs.IT]*, p. 1–37, 2013.

G.-LUERSSEN K. MORRISON, C. T. H. Cyclic Orbit Codes and Stabilizer Subfields. *Advances in Mathematics of Communications*, v. 9, p. 177–197, 2015.

GABIDULIN, E. M. Theory of Codes with Maximum Rank Distance. *Problems of Information Transmission*, v. 21, p. 1–12, 1985.

GARCíA, I. N. I. G. Some Costructions of Subspaces Cyclic and Quasi-Cyclic Codes. *Preprint arXiv:1504.04553v1.*, p. 1–10, 2015.

GAZZONI, W. C. *Estudo do Emaranhamento Quântico com Base na Teoria da Codificação Clássica.* [S.l.]: Tese de Doutorado, FEEC-UNICAMP, Campinas, SP, 2008.

GERôNIMO, J. *Extensão da Z_4-Linearidade Via Grupo de Simetrias.* [S.l.]: Tese de Doutorado, FEEC-UNICAMP, Campinas, SP, 1997.

HEFEZ, M. V. A. *Códigos Corretores de Erros.* [S.l.]: IMPA, 2002.

HUPPERT, B. *Endliche Gruppen I.* [S.l.]: Springer-Verlag, 1967.

IMAI, S. H. H. A New Multilevel Coding Method Using Error-Correcting Codes. *IEEE Transactions on Information Theory*, v. 23, p. 371–377, 1977.

JR., G. D. F. Coset Codes - Part I: Introduction and Geometrical Classification. *IEEE Transactions on Information Theory*, v. 34, p. 1123–1152, 1988.

JR., G. D. F. Geometrically Uniform Codes. *IEEE Transactions on Information Theory*, v. 37, p. 1241–1260, 1991.

KHALEGHI D. SILVA, F. R. K. A. Subspace Codes. *Lecture Notes in Computer Science*, v. 5921, p. 1–21, 2009.

KöTTER, F. K. R. Coding for Errors and Erasures in Random Network Coding. *IEEE Transactions on Information Theory*, v. 54, p. 3579–3591, 2008.

LANG, S. *Linear Algebra.* [S.l.]: Springer, 2004.

LIDL, H. N. R. *Finite Fields.* [S.l.]: Cambridge University Press, 1997.

LOELIGER, H. A. Signal Sets Matched to Groups. *IEEE Transactions on Information Theory*, v. 37, p. 1675–1682, 1991.

MACWILLIAMS, N. S. F. *The Theory of Error-Correcting Codes.* [S.l.]: The Mathematical Association of America, 1983.

MANGANIELLO, A.-L. T. F.; ROSENTHAL, J. On Conjugacy Classes of Subgroups of the General Linear Group and Cyclic Orbit Codes. *Proceedings IEEE International Symposium on Information Theory (ISIT), St. Petersburg*, 2011.

MARTIN, X. J. Z. W. J. Anticodes for the Grassmann and Bilinear Forms Graphs. *Designs, Codes and Cryptography*, v. 6, p. 73–79, 1995.

MEYER, N. R. W. D. A. Global Entaglement in Multiparticle Systems. *Journal Mathematical Physics*, v. 43, p. 4273–4278, 2002.

NIELSEN, I. L. C. M. A. *Quantum Computation and Quantum Information.* [S.l.]: Cambridge University Press, 2000.

NóBREGA, R. W. da. *Códigos de Subespaço Aplicados a Codificação de Rede.* [S.l.]: Dissertação de Mestrado, UFSC, Florianópolis, SC, 2009.

PAI, B. S. R. B. S. On the Bounds of Certain Maximal Linear Codes in a Projective Space. *IEEE Transactions on Information Theory*, v. 61, p. 4923–4927, 2015.

PERES, A. *Quantum Theory: Concepts and Methods*. [S.l.]: Kluwer Academic Publishers, 1995.

ROSENTHAL, A.-L. T. J. A Complete Characterization of Irreducible Cyclic Orbit Codes and Their Plücker Embedding. *Designs, Codes and Cryptography*, v. 66, p. 275–289, 2013.

ROTMAN, J. J. *An Introduction to the Theory of Groups*. [S.l.]: Springer-Verlag, 1995.

SCOTT, A. J. Multipartite Entanglement, Quantum Error-Correcting Codes, and Entangling Power of Quantum Evolution. *Phys. Rev. A*, v. 69, p. 052330, 2004.

SHOR, P. W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proceedings of the 35th Annual Symposium on Fundamentals of Computer Science*, 1997.

SILVA, F. K. D. On Metrics for Error Correction in Network Coding. *IEEE Transactions on Information Theory*, v. 55, p. 5479–5490, 2008.

SLEPIAN, D. Group Codes for the Gaussian Channel. *Bell System Technical Journal*, v. 47, p. 575–602, 1968.

SUPRUNENKO, D. A. *Matrix Groups*. [S.l.]: American Mathematical Society - Translations of Mathematical Monographs, 1976. v. 45.

TRAUTMANN, A.-L. *Constructions, Decoding and Automorphisms of Subspace Codes*. [S.l.]: Dissertation - Mathematisch-naturwissenschaftlichen Fakultät der Universität Zürich, 2013.

TRAUTMANN, A.-L. Isometry and Automorphisms of Constant Dimension Codes. *Advances in Mathematics of Communications*, v. 7, p. 147–160, 2013.

TRAUTMANN F. MANGANIELLO, J. R. A.-L. Orbit Codes — A New Concept in the Area of Network Coding. *IEEE Information Theory Workshop, Dublin*, 2010.

TRAUTMANN F. MANGANIELLO, M. B. J. R. A.-L. Cyclic Orbit Codes. *IEEE Transactions on Information Theory*, v. 59, p. 7386–7404, 2013.

UNGERBOECK, G. Channel Coding with Multilevel/Phase Signals. *IEEE Transactions on Information Theory*, v. 28, p. 55–67, 1982.

WAN, Z. On Geometrically Uniform Signal Sets and Signal Sets Matched to Groups. *IEEE International Symposium on Information Theory*, 1993.

WEYL, H. *The Theory of Groups and Quantum Mechanics*. [S.l.]: Dover Publisher, 1950.