JOÃO PAULO BRESSAN

LIMITANTES PARA EMPACOTAMENTOS DE ESFERAS EM VARIEDADES FLAG

CAMPINAS
2012

UNIVERSIDADE ESTADUAL DE CAMPINAS

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

JOÃO PAULO BRESSAN

LIMITANTES PARA EMPACOTAMENTOS DE ESFERAS EM VARIEDADES FLAG

Orientadora: Profa. Dra. Sueli Irene Rodrigues Costa

Tese de Doutorado apresentada ao Instituto de Matemática, Estatística e Computação Científica da UNICAMP, para a obtenção do título de Doutor em Matemática Aplicada.

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA TESE DEFENDIDA PELO ALUNO JOÃO PAULO BRESSAN, E ORIENTADA PELA PROFA. DRA. SUELI IRENE RODRIGUES COSTA.

Assinatura do Orientador:

CAMPINAS

2012

FICHA CATALOGRÁFICA ELABORADA POR
ANA REGINA MACHADO - CRB8/5467
BIBLIOTECA DO INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E
COMPUTAÇÃO CIENTÍFICA - UNICAMP

Bressan, João Paulo, 1983-
B754L Limitantes para empacotamentos de esferas em variedades flag / João Paulo Bressan. – Campinas, SP : [s.n.], 2012.

Orientador: Sueli Irene Rodrigues Costa.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria da codificação. 2. Empacotamento de esferas. 3. Espaços homogêneos. 4. Geodésia (Matemática). 5. Curvatura. I. Costa, Sueli Irene Rodrigues,1949-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em inglês: Sphere packing bounds on flag manifolds
Palavras-chave em inglês:
Coding theory
Sphere packings
Homogeneous spaces
Geodesics (Mathematics)
Curvature
Área de concentração: Matemática Aplicada
Titulação: Doutor em Matemática Aplicada
Banca examinadora:
Sueli Irene Rodrigues Costa [Orientador]
Aurelio Ribeiro Leite de Oliveira
Caio José Colletti Negreiros
Danilo Silva
Marcelo Muniz Silva Alves
Data de defesa: 20-12-2012
Programa de Pós-Graduação: Matemática Aplicada

Tese de Doutorado defendida em 20 de dezembro de 2012 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). SUELI IRENE RODRIGUES COSTA

Prof(a). Dr(a). DANILO SILVA

Prof(a). Dr(a). MARCELO MUNIZ SILVA ALVES

Prof(a). Dr(a). AURELIO RIBEIRO LEITE DE OLIVEIRA

Prof(a). Dr(a). CAIO JOSÉ COLLETTI NEGREIROS

"Tudo tem a sua ocasião própria, e há tempo para todo propósito debaixo do céu.
Há tempo de nascer, e tempo de morrer;
tempo de plantar, e tempo de arrancar o que se plantou;
tempo de matar, e tempo de curar;
tempo de chorar, e tempo de rir;
tempo de buscar, e tempo de perder;
tempo de estar calado, e tempo de falar;
tempo de guerra, e tempo de paz."

Eclesiastes, 3 : 1-8.

Agradecimentos

Registro aqui meus sinceros agradecimentos a todos aqueles que de alguma forma contribuíram para a conclusão deste trabalho.

Aos meus pais Marina e João Adevair, e meu irmão Juliano, que compartilharam minhas preocupações durante este período difícil e torceram muito para que tudo terminasse bem. Um agradecimento muito especial a minha esposa Daliane, companheira fiel que esteve ao meu lado durante todo o processo de elaboração da tese, sempre me escutando e aconselhando sabiamente quando preciso. Realmente o suporte que ela me ofereceu foi imprescindível para conclusão desse trabalho. *(Muito obrigado amor pela sua paciência, sei que não foi fácil!)*

Agradeço a todos os amigos e colegas do IMECC. Um agradecimento especial ao Linão, ou melhor, ao prof. do IMECC Lino A. S. Grama, pela ajuda preciosa na pesquisa que gerou os resultados mais relevantes desta tese. Também agradeço aos meus tios Wilson e Vilma, que sempre me acolheram em sua casa nas muitas vezes que estive em Campinas, me tratando de forma excepcional. Nada do que eu faça pode retribuir toda a ajuda que vocês me deram.

Agradeço aos professores membros da banca examinadora, pela criteriosa avaliação e pertinentes sugestões. Meus sinceros agradecimentos a minha orientadora Profa. Sueli Costa, pela oportunidade e pelo tratamento maravilhoso que me deu durante todo o tempo de pesquisa juntos, sempre demonstrando respeito e maturidade mesmo em situações adversas. Agradeço a CAPES, pela bolsa de doutorado; ao apoio financeiro da FAPESP (projeto temático 2007/56052-0); e aos colegas da UFMS - Campus de Três Lagoas, pelo efetivo apoio, em particular, na fase final da conclusão desta tese.

Finalmente agradeço a Deus, que além de continuar me dando forças para alcançar meus objetivos, me ensinou que tudo tem um tempo certo para acontecer.

Resumo

A partir das desigualdades de Hamming e Gilbert-Varshamov obtém-se um limitante superior e um limitante inferior para o número de pontos de um código numa variedade flag geométrica. Isto é feito tomando-se uma estimativa para o volume de bolas geodésicas, que resulta de cálculos envolvendo a curvatura seccional destas variedades. Em particular, são derivados limitantes para empacotamentos de esferas numa variedade de Grassmann complexa. Um limitante superior para a distância mínima também é obtido através da inversa da função que calcula o volume de um chapéu esférico. Esta técnica geométrica também é aplicada no estudo de limitantes para empacotamentos em alguns casos particulares de variedades flag maximais. Através de procedimentos computacionais, tais limitantes são implementados numericamente em alguns exemplos. Uma motivação para este trabalho foi a busca de possíveis extensões de alguns resultados sobre as grassmanianas complexas, cujo interesse na área de comunicações vem de uma interpretação que pode ser feita da transmissão em canais MIMO não coerentes via códigos em tais variedades.

Abstract

Upper and lower bounds for the number of points of codes in geometric flag manifolds are obtained from Hamming and Gilbert-Varshamov inequalities. This is done by taking an estimate for the volume of geodesic balls, as a result of calculations involving the sectional curvature of such manifolds. As a particular case, sphere packing bounds in complex Grassmann manifolds are derived. An upper bound on the minimum distance is also obtained through the inverse mapping for the volume of spherical caps. This geometric technique is also applied in the study of sphere packing bounds in some particular cases of full-flag manifolds. Such bounds are numerically implemented in some examples. One motivation for this work was the search for possible extensions of some results on complex Grassmann manifolds, which interest in communications comes from a model for the transmition on non-coherent MIMO channels via codes in such manifolds.

Sumário

Capítulo 1

Introdução

Um dos problemas fundamentais da Teoria de Códigos é o estudo da relação entre o número de pontos de um código e sua distância mínima. Em se tratando de códigos em variedades diferenciáveis, podemos destacar os *códigos esféricos* (isto é, arranjos finitos de pontos sobre a esfera $S^{n-1} \subset \mathbb{R}^n$), bastante estudados por suas aplicações, não apenas em transmissão de sinais, mas em diversas outras áreas do conhecimento. Códigos em outros tipos de variedades também vem sendo bastante estudados, não apenas por se tratar de uma generalização natural dos códigos esféricos, mas também pela descoberta de suas aplicações em alguns ramos da Teoria de Informação. A motivação deste trabalho surgiu do estudo de interessantes conexões apresentadas nos últimos anos entre cenários de comunicação *wireless* de múltiplas antenas e distribuições de pontos nas variedades de Grassmann e Stiefel complexas.

A ilustração abaixo representa um sistema genérico de comunicação [17].

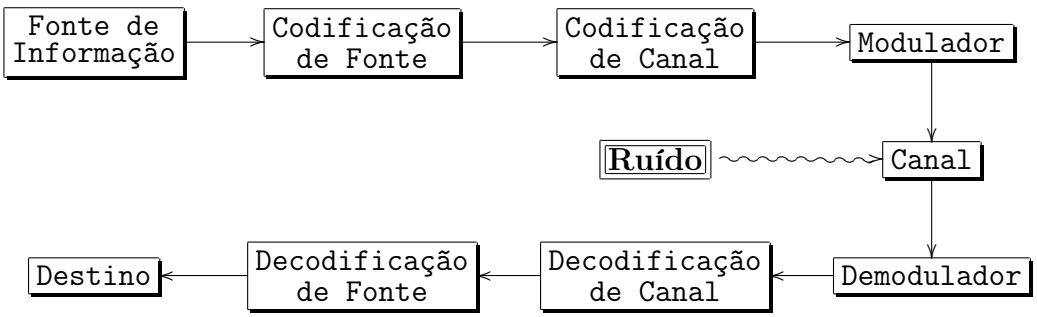

Figura 1.1: Diagrama de blocos de um sistema de comunicação.

As características específicas destes sistemas variam de acordo com o tipo de comunicação e a natureza da informação transmitida. Por exemplo, o esquema pode descrever uma conversa por telefone, a comunicação entre computadores ligados em rede, transmissões de rádio e TV, a gravação de um CD, entre outros.

Em um *sistema de comunicação digital*, a informação gerada na fonte é convertida em um *sinal digital*, isto é, uma sequência de dígitos binários. Esta primeira etapa do processo de codificação é chamada *codificação de fonte*. O objetivo da *codificação de canal* é adicionar alguma redundância na sequência de dígitos binários gerada pelo codificador de fonte. Este procedimento, de caráter sistemático e não aleatório, é feito para que o receptor possa tomar vantagem da informação redundante adicional para recuperar uma eventual sequência de informação corrompida. O *modulador* transforma a informação digital em sinais capazes de ser transmitidos através do canal. Por exemplo, se o canal do sistema é um cabo de fibra ótica então o modulador trasformará a informação digital em pontos de luz, para que assim possam viajar através da fibra. É do *canal de comunicação* que provém a conexão entre a fonte e o destino da informação. As informações precisam viajar através de um meio físico para atingir o receptor, e este meio é justamente o canal. Existem vários tipos de canais, dependendo do tipo de informação transmitida, tais como a atmosfera em transmissões sem fio, ou cabos de rede na comunicação entre computadores. Geralmente, é nesse ponto do processo de comunicação que a informação é corrompida pelo *ruído*. Contudo, convém observar que a informação também pode sofrer interferência em outras etapas. O *demodulador* detecta e estima o sinal corrompido do canal, revertendo o processo para obter um novo sinal digital. Este sinal não é necessariamente o mesmo gerado pelo codificador de canal, pois ele pode ter sofrido interferência do ruído. O *decodificador de canal* faz o processo inverso, isto é, elimina a redundância adicionada pelo codificador de canal, assumindo que o sinal que fora transmitido é o ponto mais próximo do recebido. Finalmente, o *decodificador de fonte* recupera a mensagem original.

Independentemente do tipo de canal, é razoável assumir que o ruído atua de modo incerto e/ou imprevisível. Portanto, o ruído no canal é caracterizado matematicamente por uma variável aleatória ou por um processo estocástico. Em um *canal binário simétrico* são transmitidas apenas sequências de 0's e 1's. Além disso, todos os símbolos tem a mesma probabilidade de serem recebidos errados e a probabilidade de que um símbolo recebido errado seja qualquer um dos outros é a mesma [10].

Um outro modelo comum para um canal de comunicação é o *canal de ruído aditivo*. Neste tipo de canal, o sinal transmitido é corrompido por um ruído aditivo, que é um processo estocástico bastante comum. O ruído aditivo é causado internamente pelos componentes eletrônicos que são usados para implementar o sistema de comunicação, ou por interferência encontrada na transmissão, como por exemplo, a interferência causada por outros usuários no canal. Se o ruído é introduzido primariamente por componentes eletrônicos e amplificado até o destino, ele é designado *ruído termal*. Este tipo de ruído é caracterizado matematicamente como um processo de ruído Gaussiano branco. Portanto, o modelo matemático resultante é usualmente chamado *canal AWGN*, abreviação de additive white Gaussian noise. Como este tipo de canal descreve uma grande classe de canais para sistemas implementáveis na prática, este é o modelo de canal predominantemente estudado na análise e construção de sistemas de comunicação [17].

De todas as etapas do processo de comunicação descrito acima, é na codificação/decodificação da informação que se insere a motivação principal deste trabalho. A teoria dos *códigos corretores de erros* busca maneiras de se realizar esta comunicação de forma eficiente, barata e o mais fiel possível. Um *código* é um conjunto de símbolos especiais, escolhidos para que sejam facilmente distinguíveis entre si, mesmo sob a interferência do ruído [32]. Do ponto de vista matemático, um código $\mathcal{C}$ pode ser considerado como um subconjunto finito de um espaço métrico. Para que $\mathcal{C}$ seja um bom código é conveniente que seus pontos sejam escolhidos o mais distantes possíveis uns dos outros, pois é através da distância que erros de transmissão podem ser detectados, e eventualmente, corrigidos. De um modo geral, quanto maior a distância entre seus elementos, maior será a capacidade de detecção/correção de erros do código. Códigos de Hamming, códigos esféricos, códigos LDPC, códigos turbo, códigos quânticos, entre outros; são apenas alguns exemplos. Todos diferentes quanto à natureza de seus elementos, mas desenvolvidos com o objetivo comum de atingir a maior eficácia possível na transmissão de sinais. Existem vários parâmetros de interesse usados para medir as características de um código. Alguns deles são: *taxa de informação*, *distância mínima entre pontos*, *raio de cobertura*, *kissing number*, *coeficiente de quantização*, dentre outros. Portanto, otimizar (isto é, maximizar ou minimizar) estes parâmetros, tornou-se objeto de grande interesse na pesquisa envolvendo códigos corretores de erros.

Um código em uma variedade diferenciável $\mathcal{M}$ é definido como um subconjunto

finito de pontos $\mathcal{C} \subset \mathcal{M}$. O empacotamento de esferas associado a $\mathcal{C}$ é formado pelo conjunto de esferas da variedade centradas nos pontos do código e com maior raio possível (igual à metade da distância mínima) de tal forma que duas destas esferas no máximo se tangengiam. Trataremos aqui de empacotamentos de esferas (ié. códigos) em *variedades flag* $\mathcal{F}$, especialmente nas de tipo geométrico [5]. Mais especificamente, estudaremos a relação entre a quantidade de pontos de um código em $\mathcal{F}$ e sua distância mínima. As variedades flag geométricas formam uma classe especial de espaços homogêneos compactos que engloba as *variedades de Grassmann*, pois se tratam de conjuntos formados por seqüências de subespaços encaixados. Considerando-se o grupo especial unitário $SU(n)$, composto pelas matrizes unitárias $A \in \mathbb{C}^{n\times n}$ tais que $\det(A) = 1$, a variedade flag geométrica pode ser caracterizada pelo espaço quociente

$$\mathcal{F}(n : n_1, ..., n_s) = \frac{SU(n)}{S(U(n_1) \times ... \times U(n_s))}, \tag{1.1}$$

onde $n = \sum_{i=1}^{s} n_i$. Assim a variedade de Grassmann complexa, que é definida como o conjunto dos subespaços m-dimensionais em $\mathbb{C}^{m+n}$ e tem estrutura dada pelo quociente

$$G_m(\mathbb{C}^{m+n}) = \frac{SU(m+n)}{S(U(m) \times U(n))}, \tag{1.2}$$

é um caso particular de variedade flag.

A análise de cenários de comunicação MIMO (Multiple-Input Multiple-Output) com m antenas de transmissão e $t > m$ símbolos transmitidos, revelou que esquemas de codificação relevantes podem ser descritos como coleções finitas de pontos sobre a *variedade de Grassmann complexa* $G_m(\mathbb{C}^t)$, se o canal é desconhecido pelo receptor, e na *variedade de Stiefel complexa* $V_m(\mathbb{C}^t)$, se o canal é conhecido pelo receptor [35]. Apesar de existir uma vasta literatura tratando das variedades de Grassmann ([7], [16], [33] e [34]), o problema de encontrar os melhores empacotamentos nestes espaços tem recebido pouca atenção [8]. Em [8] os autores apresentam extensos cálculos neste problema, para casos particulares em dimensões fixadas, através de um mergulho da Grassmanniana em uma esfera Euclidiana de raio e dimensão convenientes. Estes cálculos os levaram a considerar como mais adequada para a variedade de Grassmann a a definição da *distância cordal*, descrita na seção 3.2. Em [3], os autores calcularam limitantes assintóticos para distância mínima de empacotamentos nas variedades de Grassmann e Stiefel, baseados em uma expressão assintótica para o volume de bolas. A abordagem desenvolvida em [2] consiste em relacionar as variedades de Grassmann

e seus códigos associados à varios produtos de *two-points homogeneous spaces*, e assim derivar limitantes superiores para estes códigos.

Neste trabalho seguimos a interessante abordagem de estimar o volume de uma bola geodésica em uma variedade Riemanniana $(\mathcal{M}^d, \lambda)$ a partir de dados sobre sua curvatura [14]. Considerando propriedades geométricas específicas das variedades flag e peculiaridades de sua curvatura seccional, podemos derivar expressões que nos permitem encontrar limitantes para empacotamentos de esferas nestes espaços [5]. As desigualdades de *Gilbert-Varshamov* e *Hamming* serão os princípios utilizados para a obtenção destes limitantes. Se $\mathcal{M}^d$ é uma variedade diferenciável compacta, munida de uma distância topológica δ e uma medida invariante $d\nu$ (ié. o volume de uma bola métrica $B_\delta(r)$ não depende do seu centro), então os limitantes de Gilbert-Varshamov e Hamming podem ser enunciados, respectivamente, como [18]:

- Dado $\rho_0 > 0$, existe um código $\mathcal{C} \subset \mathcal{M}$ com distância mínima $\delta(\mathcal{C}) \geq \rho_0$, tal que
$$\nu\left(B_\delta\left(\rho_0\right)\right) \geq \frac{\nu(\mathcal{M})}{|\mathcal{C}|}. \tag{1.3}$$
- Para todo código $\mathcal{C} \subset \mathcal{M}$ vale
$$\nu\left(B_\delta\left(\frac{\rho_0}{2}\right)\right) \leq \frac{\nu(\mathcal{M})}{|\mathcal{C}|}. \tag{1.4}$$

Com o objetivo de calcular a curvatura seccional de um espaço homogêneo munido de uma métrica normal, iniciamos o segundo capítulo com uma descrição das propriedades fundamentais deste tipo de variedade, que por sua vez, engloba os objetos principais de nosso estudo: as variedades flag e as grassmannianas. Apresentamos mais detalhadamente a seguir as desigualdades de Hamming e Gilbert-Varshamov, que serão utilizadas na obtenção dos resultados principais do segundo capítulo. Ainda neste capítulo, descrevemos a técnica de Bishop-Gunther [14] que fornece meios de estimar o volume de uma bola geodésica em uma variedade diferenciável a partir de informações sobre sua curvatura. Esta estimativa é fundamental para o cálculo dos nossos limitantes.

No terceiro capítulo apresentamos detalhadamente alguns aspectos da geometria das variedades flag geométricas, com o objetivo principal de descrever matricialmente vetores em seu espaço tangente. Tal descrição é utilizada no cálculo da curvatura

seccional e da curvatura de Ricci destes espaços. Desse modo, podemos combinar as desigualdades de Hamming e Gilbert-Varshamov à estimativa de volume de Bishop-Gunther e estabelecer um limitante inferior e um limitante superior para o número de pontos de um código numa variedade flag geométrica [5]. Ainda, um limitante superior para a distância mínima de um código é derivado da mesma técnica, e calculado através da inversa da função que fornece o volume de um chapéu numa esfera de raio apropriado. Estes são os resultados principais deste trabalho. Finalmente estes limitantes são calculados numericamente em alguns exemplos através de procedimentos computacionais usando o programa *Wolfram - Mathematica*. Numa tentativa de estender nossos resultados, damos atenção especial na última seção ao estudo da curvatura de variedades flag maximais. A partir de um grupo de Lie complexo e simples, definimos a *variedade flag generalizada* via a decomposição da álgebra de Lie associada em espaços de raízes. Fixada uma base de Weyl, obtemos uma fórmula para a curvatura de Ricci destas variedades no caso maximal, que depende exclusivamente das constantes de estrutura da álgebra. Mostramos ainda que esta nova fórmula, quando restrita às variedades flag geométricas, coincide com a expressão encontrada na seção anterior.

No quarto capítulo descrevemos a caracterização apresentada em [35] da capacidade de canais de múltiplas antenas (MIMO) com desvanecimento de Rayleigh no caso não-coerente (onde os coeficientes de desvanecimento são desconhecidos pelo receptor) via empacotamentos de esferas na variedade de Gramssmann complexa. Este estudo, que foi a principal motivação deste trabalho, é baseado no modelo introduzido em [20] envolvendo matrizes complexas, e utilizando uma mudança de coordenadas $\mathbb{C}^{m\times t} \longrightarrow \mathbb{C}^{m\times m} \times G_m(\mathbb{C}^t)$. Na seção 4.1 observamos a existência de uma mudança de coordenadas alternativa $\mathbb{C}^{m\times t} \longrightarrow U^{m\times m} \times \mathcal{F}$, onde $U^{m\times m}$ denota o conjunto das matrizes triangulares superiores de tamanho $m \times m$ e $\mathcal{F}$ é uma variedade flag geométrica apropriada. Já na seção 4.2 damos atenção especial ao estudo de distâncias na variedade de Grassmann e também ao *mergulho esférico*, utilizado na definição da *distância cordal*. Além disso, descrevemos o mergulho de uma variedade flag generalizada numa variedade de Grassmann, com o objetivo de obter uma definição semelhante da distância cordal também para as variedades flag.

No apêndice nos dedicamos à síntese dos resultados que julgamos necessários como pré-requisito para um bom entendimento do estudo desenvolvido nos capítulos anteriores. Como utilizamos no trabalho uma boa quantidade de conhecimentos em

geometria, o apêndice apresenta uma introdução à teoria de Lie, tanto álgebras como grupos. As demonstrações das proposições e teoremas são omitidas, porém indicadas na bibliografia.

Nossa abordagem aqui é essencialmente teórica. Ou seja, não sabemos ainda se existem sistemas de comunicação implementáveis que sejam bem caracterizados por códigos em variedades flag diferentes das grassmannianas, mas acreditamos que esta é uma investigação bem pertinente. Cabe também ressaltar que este tipo de variedade tem sido objeto de interesse na pesquisa de diversas subáreas da matemática e da física, de onde surgem resultados relevantes.

Capítulo 2

Códigos em Espaços Homogêneos

Neste capítulo introduzimos os espaços homogêneos, os quais incluem as variedades flag, e descrevemos propriedades fundamentais para a obtenção dos resultados que serão apresentados no decorrer do trabalho. As principais referências utilizadas foram [6], [14], [24], [29] e [30]. A ênfase será o estudo da curvatura seccional destes espaços, cuja expressão será muito importante na obtenção dos limitantes apresentados no próximo capítulo. Também enunciaremos o *teorema de Bishop-Gunther*, que será utilizado no capítulo 2 para a obtenção de uma estimativa para o volume de uma bola geodésica numa variedade flag, estendendo assim a abordagem feita em [18].

Do ponto de vista matemático, um *código* $\mathcal{C}$ é um subconjunto finito de pontos em um espaço métrico (X, δ). Dentro das infinitas possibilidades e por alguma razão, é necessário escolher uma distância δ que seja interessante, pois esta implicará diretamente nas propriedades do código. Por exemplo, em sua capacidade de detectar e/ou corrigir erros, uma característica de extrema importância. Uma métrica riemanniana λ numa variedade diferenciável $\mathcal{M}$ é dada por uma escolha de produtos internos nos espaços tangentes em cada ponto. Sob certas hipóteses λ induz em $\mathcal{M}$ uma distância geodésica δ_g, e as variedades do tipo $(\mathcal{M}, \delta_g)$ constituirão a classe especial de espaços métricos que consideraremos. Mais ainda, neste capítulo os espaços métricos onde habitam os códigos serão espaços homogêneos compactos do tipo $\mathcal{M} = G/H$ munidos da distância geodésica proveniente de uma métrica normal. A homogeneidade se deve à necessidade de uma invariância das estruturas do espaço por isometrias, como por exemplo, o fato do volume das bolas não depender de seu centro mas apenas de seu raio. Esta invariância será um fator fundamental na demonstração dos resultados

principais do próximo capítulo.

Na seção 2.1 sintetizamos conceitos e resultados básicos sobre a geometria dos espaços homogêneos, com o objetivo principal de determinar uma expressão explícita para a curvatura seccional destes espaços. Na seção 2.2 apresentamos algumas considerações gerais da teoria de códigos em variedades diferenciáveis. Na seção 2.3 descrevemos teoricamente os limitantes de Hamming e Gilbert-Varshamov para o número máximo e mínimo de pontos de um código, cujos cálculos serão desenvolvidos no próximo capítulo. Veremos então que tal desenvolvimento demanda um bom conhecimento do volume de bolas geodésicas na variedade que contém os códigos. Por este motivo, na seção 2.4, damos uma breve introdução à técnica de Bishop-Gunther para estimar volumes de bolas geodésicas a partir de informações sobre a curvatura.

2.1 Espaços Homogêneos

2.1.1 Resultados e Conceitos Básicos

Espaços homogêneos são variedades diferenciáveis $\mathcal{M}$ que sofrem a ação transitiva de um grupo de Lie conexo G. Eles constituem uma classe especial de variedades, e de certo modo, pode-se dizer que os espaços homogêneos são os exemplos mais tratáveis de variedades Riemannianas. De fato, a ação de G nos permite definir o conceito de invariância de uma métrica em $\mathcal{M}$, e desse modo, a geometria desses espaços simplifica-se de modo substancial. Em suma, características importantes de um espaço homogêneo podem ser totalmente descritas apenas conhecendo-as na vizinhança de algum de seus pontos. Mais detalhes deste tema e as demonstrações das proposições presentes nesta seção podem ser encontrados em [6], [24] e [29]. Alguns conceitos e resultados preliminares da teoria de grupos e álgebras de Lie, que podem tornar a leitura dessa seção mais confortável, são apresentados no apêndice A.

Definição 2.1.1 *Uma* **ação** *(à esquerda) de um grupo G numa variedade diferenciável $\mathcal{M}$ é uma aplicação*

$$\Phi : G \times \mathcal{M} \longrightarrow \mathcal{M}, \tag{2.1}$$

que associa a cada $g \in G$ uma função $\Phi_g : \mathcal{M} \longrightarrow \mathcal{M}$ tal que:

- $\Phi_1 = I_{\mathcal{M}}$, *isto é,* $\Phi_1(p) = p,\ \forall p \in \mathcal{M}$;

- $\Phi_{gh} = \Phi_g \circ \Phi_h, \ \forall g, h \in G.$

Visto que $I_{\mathcal{M}} = \Phi_1 = \Phi_{gg^{-1}} = \Phi_g \circ \Phi_{g^{-1}}$ e $I_{\mathcal{M}} = \Phi_{g^{-1}} \circ \Phi_g$, segue que cada função Φ_g é uma bijeção de $\mathcal{M}$. Desse modo, cada ação à esquerda é um homomorfismo $\Phi : G \longrightarrow B(\mathcal{M})$, onde $B(\mathcal{M})$ denota o grupo das bijeções de $\mathcal{M}$. Substituindo a segunda propriedade da definição acima por $\Phi_{gh} = \Phi_h \circ \Phi_g$, podemos definir uma *ação à direita* de um grupo G sobre uma variedade $\mathcal{M}$. Aqui trataremos apenas de ações de grupo à esquerda, e diremos apenas se tratar de uma *ação* de G sobre $\mathcal{M}$. Ainda, por conveniência de notação, escreveremos apenas $g(x)$ ao invés de $\Phi_g(x)$.

Definição 2.1.2 *Se um grupo G age sobre uma variedade $\mathcal{M}$, então dado $p \in \mathcal{M}$ definimos sua* **órbita** *como*

$$O_p = \{g(p) \in \mathcal{M} : g \in G\}, \tag{2.2}$$

e seu **subgrupo de isotropia** *(ou estabilizador) como*

$$G_p = \{g \in G : g(p) = p\}. \tag{2.3}$$

O subgrupo de isotropia é de fato um subgrupo de G, visto que dados $g, h \in G_p$ temos $(gh)(p) = g(h(p)) = g(p) = p$, pois g e h fixam p. Além disso, $g^{-1}(p) = \Phi_{g^{-1}}(p) = \Phi_g^{-1}(p) = p$ pois g leva p em p. Observe que o subgrupo de isotropia G_p da ação é o conjunto formado por todas as aplicações $\Phi_g : \mathcal{M} \longrightarrow \mathcal{M}$ que tem p como ponto fixo.

Definição 2.1.3 *Uma ação de G sobre $\mathcal{M}$ é dita* **transitiva** *se, para quaisquer $p, q \in \mathcal{M}$, existe $g \in G$ tal que $g(p) = q$.*

Observe que se a ação (2.1) é transitiva, então $O_p = \mathcal{M}$, qualquer que seja $p \in \mathcal{M}$. Isto é, a órbita de qualquer elemento é toda a variedade.

Considere agora H um subgrupo de G. De modo usual, podemos definir a relação de equivalência em G

$$g_1 \simeq g_2 \ \Leftrightarrow \ g_1^{-1} g_2 \in H, \quad \forall g_1, g_2 \in G. \tag{2.4}$$

Segue imediatamente que a classe de equivalência de um elemento $g \in G$ é dada por

$$gH = \{gh : h \in H\}. \tag{2.5}$$

O conjunto formado pelas classes de equivalência da relação (2.4) é chamado de *conjunto quociente*, e será denotado G/H. Isto é,

$$G/H = \{gH : g \in G\}. \tag{2.6}$$

Ainda, temos bem definida a aplicação sobrejetiva, denominada *projeção canônica*,

$$\pi : G \longrightarrow G/H \tag{2.7}$$

que faz corresponder a cada elemento $g \in G$ a respectiva classe de equivalência gH. É um fato bastante conhecido que G/H admite uma estrutura de grupo com operação induzida por G se, e somente se, H for um *subgrupo normal*. Mais detalhes sobre grupos quocientes podem ser encontrados em textos de álgebra, tais como [19].

Definição 2.1.4 *Se G é um grupo de Lie conexo e H um subgrupo fechado de G, então o conjunto quociente G/H é chamado de* **espaço homogêneo**.

O grupo G age naturalmente à esquerda no espaço homogêneo G/H através da aplicação $\Phi : G \times G/H \longrightarrow G/H$ definida por

$$\Phi(g, g_1H) := (gg_1)H. \tag{2.8}$$

Fixado um elemento $g \in G$, sabemos que esta ação induz uma bijeção $L_g = \Phi(g, *)$ em G/H, denotada simplesmente por g. Observe que (2.8) é uma ação transitiva pois, dados $p, q \in G/H$ com $p = g_1H$ e $q = g_2H$, basta tomar $g = g_2g_1^{-1} \in G$ e teremos

$$g(p) = (gg_1)H = (g_2g_1^{-1}g_1)H = g_2H = q.$$

Nesse caso, como observado anteriormente, a órbita de qualquer ponto $p \in G/H$ é todo G/H.

Proposição 2.1.1 *[29] Existe uma única estrutura diferenciável no espaço homogêneo G/H que é compatível com a topologia quociente. Munido desta estrutura, a ação natural (2.8) é diferenciável (consequentemente cada bijeção $g : G/H \longrightarrow G/H$ é um difeomorfismo) e a projeção canônica (2.7) é uma submersão sobrejetora.*

Reciprocamente, suponha que $\mathcal{M}$ é uma variedade diferenciável e que

$$\Phi : G \times \mathcal{M} \longrightarrow \mathcal{M}$$

é a ação transitiva de um grupo de Lie conexo G em $\mathcal{M}$. Se esta ação for diferenciável (particularmente ela é contínua) então, qualquer que seja $p \in \mathcal{M}$, seu subgrupo de isotropia G_p é fechado em G. De fato, $G_p = \Phi^{-1}(\{p\})$ e $\{p\}$ é fechado em $\mathcal{M}$, pois toda variedade diferenciável é um *espaço topológico de Hausdorff*. Desse modo G_p é um subgrupo de Lie de G, qualquer que seja $p \in \mathcal{M}$.

Podemos identificar o quociente de G por um subgrupo de isotropia G_p com a órbita O_p. Para isso basta ver que a aplicação

$$\psi : G/G_p \longrightarrow O_p \tag{2.9}$$

definida por $\psi(gG_p) = g(p)$ é uma bijeção. Sendo Φ uma ação transitiva, para todo $p \in \mathcal{M}$ temos $O_p = \mathcal{M}$, e vale o seguinte resultado.

Proposição 2.1.2 *[29] Considere uma ação transitiva diferenciável de um grupo de Lie conexo G em uma variedade $\mathcal{M}$. Então, qualquer que seja $p \in \mathcal{M}$, a aplicação (2.9) é um difeomorfismo. Portanto, $\mathcal{M}$ admite a estrutura de espaço homogêneo $\mathcal{M} = G/G_p$.*

Queremos estudar métricas em G/H para as quais o grupo G age por isometrias. Tais métricas são ditas invariantes, e serão definidas a seguir.

Definição 2.1.5 *Uma métrica Riemanniana λ num espaço homogêneo $\mathcal{M} = G/H$ é dita* **invariante à esquerda** *se cada difeomorfismo da ação (2.8) é uma isometria. Isto é, para todo $p \in \mathcal{M}$ vale*

$$\lambda(X, Y)_p = \lambda(dg(X), dg(Y))_{g(p)}, \ \forall X, Y \in T_p\mathcal{M}. \tag{2.10}$$

Particularmente, ao tomarmos o próprio grupo G como espaço homogêneo, podemos também considerar a ação à direita de G nele mesmo. Nesse caso especial, uma métrica invariante por ambas as ações, à esquerda e à direita, será chamada *bi-invariante*. Nesse ponto é importante observarmos que nem todo espaço homogêneo admite uma métrica invariante (veja [6]). Além disso, quando um espaço homogêneo G/H admite uma métrica invariante, o grupo G pode não conter todas as isometrias

de G/H.

Sabemos que se H é um subgrupo de Lie de G, então $\mathfrak{h} = \mathfrak{Lie}(H)$ é uma subálgebra de Lie de $\mathfrak{g}$. O espaço tangente de qualquer ponto num espaço homogêneo G/H pode ser naturalmente identificado com $\mathfrak{m} = \mathfrak{h}^{\perp}$, o complementar ortogonal de $\mathfrak{h}$ em $\mathfrak{g}$ em relação à *forma de Cartan-Killing*. Temos então a decomposição

$$\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{m}, \tag{2.11}$$

e assim um vetor $X \in \mathfrak{g}$ pode ser escrito de modo único como $X = X_{\mathfrak{h}} + X_{\mathfrak{m}}$.

Proposição 2.1.3 *[6] O conjunto das métricas invariantes num espaço homogêneo G/H é isomorfo ao conjunto dos produtos internos Ad-invariantes em $\mathfrak{m}$.*

Se a métrica $\langle\ ,\ \rangle$ de G é bi-invariante, então sua restrição $\langle\ ,\ \rangle|_{\mathfrak{m}}$ será chamada de *métrica normal* em G/H. Quando a métrica em G/H é normal, diremos que G/H é um *espaço homogêneo normal*.

Exemplo 2.1.1 (A Esfera n-dimensional) *O grupo especial ortogonal*

$$SO(n) = \{A \in I\!R^{n\times n} : AA^t = I_n \text{ e } \det(A) = 1\}$$

é um grupo de Lie compacto e conexo que age transitivamente sobre a **esfera unitária**

$$S^{n-1} = \{x = (x_1, ..., x_n) \in I\!R^n : \sum_{i=1}^{n} x_i^2 = 1\}$$

por multiplicação à esquerda $\Phi_A(x) = Ax$. De fato, se $x \in S^{n-1}$ e $A \in SO(n)$ então $Ax \in S^{n-1}$ pois $\|Ax\|^2 = \|x\|^2 = 1$. Além disso, dados dois pontos $x, y \in S^{n-1}$ sempre é possível encontrar uma matriz ortogonal A com determinante 1 tal que $Ax = y$. Observando que o estabilizador desta ação é isomorfo a $SO(n-1)$, segue pela Proposição 1.1.2 que a esfera admite estrutura de espaço homogêneo

$$S^{n-1} = SO(n)/SO(n-1). \tag{2.12}$$

A métrica normal em $SO(n)$ é dada por

$$\langle X, Y\rangle_N = \mathrm{tr}(XY^t),$$

para quaisquer $X, Y \in \mathfrak{so}(n) = T_{I_n}(SO(n))$. *Assim, a norma de um vetor tangente coincide com a norma Euclidiana*

$$\|X\|^2 = \mathrm{tr}(XX^t) = \sum_{i=1}^{n} x_i^2. \ \square$$

2.1.2 Curvatura

Nosso objetivo a partir de agora será calcular a curvatura de um espaço homogêneo G/H com a métrica normal. Como veremos na seção 2.4, conhecer a curvatura de G/H será essencial para obtermos estimativas de volume de uma bola geodésica em G/H a partir do teorema de Bishop-Gunther. A partir disso, será possível encontrar limitantes na distância mínima e no tamanho de um código contido em uma variedade com estrutura de espaço homogêneo. Particularmente, estamos interessados em obter resultados para Grassmannianas e variedades flag. A proposição seguinte trata do caso particular em que G/H é o próprio grupo G. Este resultado, juntamente ao *teorema de O'Neill*, será utilizado para obter a expressão da curvatura seccional K de um espaço homogêneo qualquer.

Para X e Y vetores no espaço tangente de uma variedade riemanniana $(\mathcal{M}, \lambda)$, a curvatura seccional $K(X, Y)$ é definida como a curvatura da superfície (subvariedade 2-dimensional) associada ao plano gerado por $\{X, Y\}$. Veremos a seguir que no caso especial de um grupo de Lie com uma métrica bi-invariante, o valor da curvatura seccional é dado apenas em função do colchete de Lie da álgebra (isto é, espaço tangente) associada.

Proposição 2.1.4 *[6] Se* $(G, \langle\ ,\ \rangle)$ *é um grupo de Lie munido de uma métrica bi-invariante , então*

$$K(X, Y) = \frac{1}{4}\|[X, Y]\|^2. \tag{2.13}$$

Em particular, a curvatura seccional de G *é não negativa.*

Podemos aplicar a proposição acima a todo grupo de Lie compacto, pois os grupos nesta classe sempre admitem uma métrica bi-invariante ([6], Prop. 3.16).

Uma *submersão* é uma aplicação diferenciável $\sigma : \mathcal{M}^{n+k} \longrightarrow \mathcal{N}^n$ tal que a diferencial $d\sigma_p$ tem posto n, para todo $p \in \mathcal{M}$. Segue pelo teorema da função implícita

que $\sigma^{-1}(p)$ é uma subvariedade k-dimensional de $\mathcal{M}$, qualquer que seja $p \in \mathcal{M}$. Se V denota o espaço tangente de $\sigma^{-1}(p)$ em algum ponto q, então o espaço tangente $T_q\mathcal{M}$ admite a decomposição

$$T_q\mathcal{M} = V \oplus V^{\perp} := V^v \oplus V^h, \tag{2.14}$$

onde V^v e V^h são denominados, respectivamente, subespaços *vertical* e *horizontal* de $T_q\mathcal{M}$. Desse modo, um vetor $X \in T_q\mathcal{M}$ se decompõe de modo único como soma de uma componente vertical e uma componente horizontal

$$X = X^v + X^h. \tag{2.15}$$

Se $d\sigma|_{V^h}$ é uma isometria, então σ será chamada de *submersão riemanniana*. Se X é um campo de vetores em $\mathcal{N}$, então existe um único campo de vetores $\tilde{X} \in V^h$ em $\mathcal{M}$ tal que $d\sigma(\tilde{X}) = X$. O campo $\tilde{X}$ é chamado de *levantamento horizontal* de X [24].

O próximo teorema relaciona a curvatura seccional de uma seção plana $K_{\mathcal{M}}(\tilde{X}, \tilde{Y})$ gerada pelos levantamentos $\tilde{X}, \tilde{Y} \in T(\mathcal{M})$ com a curvatura seccional do plano gerado por $X, Y \in T(\mathcal{N})$.

Teorema 2.1.1 (O'Neill) *Se $\sigma : \mathcal{M} \longrightarrow \mathcal{N}$ é uma submersão riemanniana, então a curvatura seccional de $\mathcal{N}$ é dada por*

$$K_{\mathcal{N}}(X, Y) = K_{\mathcal{M}}(\tilde{X}, \tilde{Y}) + \frac{3}{4}\|[\tilde{X}, \tilde{Y}]^v\|^2, \tag{2.16}$$

onde X, Y são campos de vetores ortonormais em $\mathcal{N}$.
Demonstração: [6], Teo. 3.20. ■

Agora estamos prontos para calcular a curvatura de um espaço homogêneo G/H com a métrica normal.

Corolário 2.1.1 *[6] Se G/H é um espaço homogêneo com uma métrica normal, então sua curvatura seccional é dada por*

$$K(X, Y) = \frac{1}{4}\|[X, Y]_{\mathfrak{m}}\|^2 + \|[X, Y]_{\mathfrak{h}}\|^2. \tag{2.17}$$

Particularmente, a curvatura seccional é sempre não negativa.
Demonstração: *A proposição 1.1.1 garante que a projeção $\pi : G \longrightarrow G/H$ é uma*

submersão. A decomposição $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{m}$ *corresponde precisamente à decomposição* $V_v \oplus V_h$ *dada em (2.14). Como a métrica* $\langle\ ,\ \rangle_N$ *de* G/H *é normal, segue que* $\langle\ ,\ \rangle_N = \langle\ ,\ \rangle|_{\mathfrak{m}}$*, onde* $\langle\ ,\ \rangle$ *é uma métrica bi-invariante de* G*. Portanto,* π *é uma submersão Riemanniana. Dados vetores ortonormais* $X, Y \in \mathfrak{m}$*, segue de (2.16) que*

$$K(X,Y) = K_G(\tilde{X},\tilde{Y}) + \frac{3}{4}\|[\tilde{X},\tilde{Y}]_{\mathfrak{h}}\|^2.$$

Observando que $\tilde{X} = X$ *e* $\tilde{Y} = X$*, pois* X *e* Y *são vetores horizontais, obtemos de (2.13) que*

$$K(X,Y) = \frac{1}{4}\|[X,Y]\|^2 + \frac{3}{4}\|[X,Y]_{\mathfrak{h}}\|^2.$$

Decompondo o colchete na soma ortogonal $[X,Y] = [X,Y]_{\mathfrak{h}} + [X,Y]_{\mathfrak{m}}$ *temos*

$$K(X,Y) = \frac{1}{4}\left(\|[X,Y]_{\mathfrak{h}}\|^2 + \|[X,Y]_{\mathfrak{m}}\|^2\right) + \frac{3}{4}\|[X,Y]_{\mathfrak{h}}\|^2$$

$$\Rightarrow \quad K(X,Y) = \frac{1}{4}\|[X,Y]_{\mathfrak{m}}\|^2 + \|[X,Y]_{\mathfrak{h}}\|^2. \ \blacksquare$$

2.2 Códigos em Espaços Homogêneos

Neste capítulo consideraremos $\mathcal{M} = G/H$ um espaço homogêneo, dado pelo quociente de um grupo de Lie compacto e conexo G por um subgrupo fechado H. Nessas condições, sabemos que G admite uma métrica bi-invariante $\langle\ ,\ \rangle$, e assim consideraremos a métrica normal induzida $\langle\ ,\ \rangle_N = \langle\ ,\ \rangle|_{\mathfrak{m}}$ em $\mathcal{M}$. Observe que a compacidade de G implica que $\mathcal{M}$ também é uma variedade diferenciável compacta.

Em geral, se $(\mathcal{M}^d, \lambda)$ é uma variedade riemanniana d-dimensional, então para cada ponto $p \in \mathcal{M}$ está definido um produto interno λ_p no espaço tangente $T_p\mathcal{M}$. Portanto, dado um vetor tangente $X \in T_pM$, podemos calcular sua norma $\|X\| = \lambda_p(X,X)^{\frac{1}{2}}$. Consequentemente, definimos a *distância geodésica* δ_g em $\mathcal{M}$ do seguinte modo: para quaisquer $p,\ q \in \mathcal{M}$, considere o conjunto $\Gamma_{p,q}$ de todas as curvas diferenciáveis $\gamma : [0,1] \longrightarrow \mathcal{M}$ ligando estes dois pontos. Sabendo que o comprimento de $\gamma \in \Gamma_{p,q}$ é dado por

$$l(\gamma) = \int_0^1 \left\|\gamma'(t)\right\| dt,$$

definimos

$$\delta_g(p,q) := \inf_{\gamma\in\Gamma_{p,q}} \{l(\gamma)\}.$$

Supondo que $\mathcal{M}$ é uma variedade compacta, segue do *teorema de Hopf-Rinow* que sempre existe uma geodésica que realiza a distância entre quaisquer dois de seus pontos, e neste caso, dizemos que $\mathcal{M}$ é uma variedade *completa*.

Particularmente, se $\mathcal{M} = G/H$ é um espaço homogêneo normal e $g : \mathcal{M} \longrightarrow \mathcal{M}$ é uma de suas isometrias, então

$$\delta_g(p,q) = \delta_g(g(p), g(q)),$$

para quaisquer $p, q \in \mathcal{M}$. De fato, se $\gamma : [0,1] \longrightarrow \mathcal{M}$ é uma curva diferenciável tal que $\gamma(0) = p$ e $\gamma(1) = q$, então $\alpha = g \circ \gamma$ é uma curva diferenciável em $\mathcal{M}$ tal que $\alpha(0) = g(p)$ e $\alpha(1) = g(q)$. Além disso, segue pela invariância da métrica que

$$l(\alpha) = \int_0^1 \left\| (g\circ\gamma)'(t) \right\| dt = \int_0^1 \langle (dg(\gamma'(t)), dg(\gamma'(t))\rangle^{\frac{1}{2}} dt =$$

$$= \int_0^1 \langle (\gamma'(t), \gamma'(t)\rangle^{\frac{1}{2}} dt = \int_0^1 \left\| \gamma'(t) \right\| dt = l(\gamma).$$

Desse modo, se $B_p(\rho) = \{x \in \mathcal{M} : \delta_g(p,x) < \rho\}$ denota a *bola geodésica aberta* de centro $p \in \mathcal{M}$ e raio $\rho > 0$, então $B_{g(p)}(\rho) = g(B_p(\rho))$. Isto implica que, com a métrica normal, as bolas geodésicas em G/H são obtidas umas das outras por meio de isometrias.

Finalmente, lembramos que para toda variedade homogênea $\mathcal{M} = G/H$ existe uma única (a menos de produto por número positivo) medida $d\nu$, que é invariante por isometrias. Desse modo, para qualquer subconjunto mensurável $S \subseteq \mathcal{M}$, temos

$$\nu(S) = \nu(g(S)), \tag{2.18}$$

para todo $g \in G$. Além disso, da hipótese de $\mathcal{M}$ ser compacta segue que $\nu(\mathcal{M}) < \infty$, e consequentemente $\nu(S) < \infty$, para qualquer $S \subseteq \mathcal{M}$ mensurável. Feitas estas observações, consideraremos a seguir códigos em espaços homogêneos.

Definição 2.2.1 *Sejam G um grupo de Lie compacto e conexo, e $\mathcal{M} = G/H$ um espaço homogêneo normal, munido da distância geodésica δ_g. Um* **código** *em $\mathcal{M}$ é*

qualquer subconjunto finito $\mathcal{C} \subset \mathcal{M}$. Um elemento $x \in \mathcal{C}$ é chamado **palavra-código**, *e o número de palavras-código $|\mathcal{C}|$ é chamado* **tamanho do código**. *A* **taxa binária de informação** *do código é definida por*

$$R(\mathcal{C}) := \frac{\log_2(|\mathcal{C}|)}{d}, \tag{2.19}$$

onde d é a dimensão de $\mathcal{M}$. A **distância mínima** *do código $\mathcal{C}$ é dada por*

$$\delta(\mathcal{C}) := \min_{x \neq y}\{\delta_g(x, y)\}, \text{ para } x, y \in \mathcal{C}. \tag{2.20}$$

Exemplo 2.2.1 (Códigos Esféricos) *Qualquer subconjunto finito de pontos na esfera unitária Euclidiana $S^{n-1} \subset \mathbb{R}^n$ é chamado de* **código esférico** *n-dimensional. O problema de alocar um conjunto finito de pontos sobre a superfície de uma esfera tem atraído a atenção de matemáticos, engenheiros e cientistas em geral, devido sua relevância em muitas áreas. As aplicações incluem transmissão de sinais, quantização esférica, avaliação numérica de integrais sobre esferas, cálculo de distribuição de cargas de energia mínima sobre a esfera, aplicações em física, química, arquitetura, entre outros [32].*

Um fato importante sobre códigos esféricos, que justifica a terminologia alternativa **constelação de sinais**, *é que todo conjunto de sinais contínuos pode ser representado por um número de pontos na esfera S^1. Este procedimento recebe o nome de* **M-PSK**, *sigla oriunda da língua inglesa para Phase-Shift Keying. Dado um conjunto de sinais $S = \{s_1(t), ..., s_M(t)\}$ formado por funções reais contínuas de energia finita (isto é, $\int_{-\infty}^{+\infty} |s_i(t)|\, dt < \infty$, para todo $i = 1, ..., M$), o gerado de S é um subespaço vetorial de dimensão finita do espaço vetorial das funções reais de energia finita, munido do produto interno usual*

$$\langle f, g\rangle = \int_{-\infty}^{+\infty} f(t)g(t)d.t$$

Desse modo, podemos construir uma base ortonormal através do processo de Gram-Schmidt, cujas colunas da matriz de passagem são vetores na esfera unitária. Mais detalhes sobre a representação geométrica de sinais podem ser encontrados no capítulo 3 de [10].

Em geral, dada uma dimensão n e um número de pontos M, um problema fundamental é descobrir qual o código esférico $[M, n]$ com maior distância mínima. Um

código com esta propriedade é chamado **ótimo**. *Configurações ótimas de pontos são muito difíceis de se encontrar, até mesmo em dimensões pequenas. Por exemplo, para* $n = 3$ *são conhecidos apenas os casos* $M \leq 12$ *e* $M = 24$ *[25]. Todas as outras são as "melhores conhecidas", sem uma prova formal de que são ótimas.* □

2.3 Limitantes de Hamming e Gilbert-Varshamov

Estamos interessados em realizar um estudo clássico da teoria de códigos, a saber, investigar a relação existente entre o tamanho de um código $|\mathcal{C}|$ e sua distância mínima $\delta(\mathcal{C})$. Neste trabalho, tal estudo é feito através de cálculos computacionais baseados nos limitantes que serão descritos teoricamente a seguir.

Vamos assumir daqui em diante que $\mathcal{M}$ é uma variedade compacta, sem fronteira, com uma distância invariante δ e uma medida invariante $d\nu$. Dado $\rho > 0$, suponha que $B_x(\rho)$ denote a bola aberta em $\mathcal{M}$ centrada no ponto x e raio ρ. Como $\mathcal{M}$ é compacta, a cobertura $\bigcup_{x\in\mathcal{M}} B_x(\rho)$ admite uma subcobertura finita $\bigcup_{i=1}^{l} B_{x_i}(\rho)$, para algum $l > 0$. Para obter estimativas, gostaríamos de calcular o volume de uma bola $B_x(\rho)$. Sabendo que a medida das bolas depende apenas de seu raio e não de seu centro, vamos usar a notação $B(\rho)$ para designar uma bola genérica de raio ρ em $\mathcal{M}$. Pelo argumento anterior, segue que dado um raio $\rho > 0$ existe um número inteiro $l > 0$ tal que

$$l\nu(B(\rho)) \geq \nu(\mathcal{M}).$$

Assim, os centros $\{x_i\}$ das bolas da cobertura finita formam um código $\mathcal{C}$, de tamanho $|\mathcal{C}| = l$. Vamos agora enunciar este princípio, chamado limitante de Gilbert-Varshamov.

Proposição 2.3.1 (Limitante Inferior de Gilbert-Varshamov [18]) *Dado* $\rho > 0$, *existe um código* $\mathcal{C} \subset \mathcal{M}$ *com distância mínima* $\delta(\mathcal{C}) \geq \rho$ *e tal que*

$$|\mathcal{C}| \geq \frac{\nu(\mathcal{M})}{\nu(B(\rho))} := L. \tag{2.21}$$

Por outro lado, é claro que para todo código $\mathcal{C} = \{x_1, ..., x_l\}$ em $\mathcal{M}$, as bolas de raio $\rho = \frac{\delta(\mathcal{C})}{2}$ centradas nos pontos de $\mathcal{C}$ não cobrem toda a variedade $\mathcal{M}$. Assim,

obtemos nossa segunda estimativa.

Proposição 2.3.2 (Limitante Superior de Hamming [18]) *Para qualquer código $\mathcal{C} \subset \mathcal{M}$ vale a desigualdade*

$$|\mathcal{C}| \leq \frac{\nu(\mathcal{M})}{\nu\left(B\left(\frac{\delta(\mathcal{C})}{2}\right)\right)} := U. \tag{2.22}$$

Desse modo, ficam explícitos um limitante inferior e um limitante superior (respectivamente, L e U) na quantidade máxima de pontos que podem ser colocados na variedade $\mathcal{M}$, de modo que a distância entre quaisquer dois pontos distintos seja maior ou igual a ρ.

Exemplo 2.3.1 (O Limitante da União) *Dados dois pontos $x, y \in S^{n-1}$, sabemos que o ângulo θ entre eles obedece a relação*

$$\cos(\theta) = \frac{\langle x, y\rangle}{\|x\|\|y\|} = \langle x, y\rangle,$$

e portanto $\theta = \cos^{-1}(\langle x, y\rangle)$. Se d é a distância entre tais pontos medida em $\mathbb{R}^n$, podemos calcular

$$\theta = 2\text{sen}^{-1}\left(\frac{d}{2}\right). \tag{2.23}$$

Dado um ponto $x \in S^{n-1}$, definimos o **chapéu esférico** *de centro x e raio $\phi \in [0, \pi]$ como o conjunto dos pontos da esfera S^{n-1} cuja separação angular de x é menor que ϕ. Denotaremos este conjunto por*

$$C_x(n, \phi) = \left\{\ y \in S^{n-1} : \langle x, y\rangle > \cos(\phi)\right\}. \tag{2.24}$$

Claramente a área de um chapéu independe de seu centro, e pode ser calculada pela fórmula [12]

$$A\left(C(n, \phi)\right) = a_{n-1}\int_0^{\phi} \text{sen}^{n-2}(\alpha)d\alpha, \tag{2.25}$$

onde

$$a_n = \begin{cases} \frac{(2\pi)^{n/2}}{(n-2)!!}, & \text{se } n = 2, 4, 6, ... \\ \\ \frac{2(2\pi)^{(n-1)/2}}{(n-2)!!}, & \text{se } n = 1, 3, 5, ... \end{cases},$$

onde o duplo fatorial de um inteiro positivo é definido recursivamente por

$$n!! = \begin{cases} 1, \text{ se } n = 0 \text{ ou } n = 1 \\ n(n-2)!!, \text{ se } n \geq 2 \end{cases}.$$

Particularmente, a área total da superfície esférica é dada por

$$A(C(n,\pi)) = \begin{cases} \frac{(2\pi)^m}{(2m-2)!!}, & \text{se } n = 2m \\ \\ \frac{2(2\pi)^m}{(2m-1)!!}, & \text{se } n = 2m+1 \end{cases}.$$

Feitas estas considerações, podemos enunciar o limitante de Hamming (2.22), que no caso particular de códigos esféricos, também é conhecido como o **limitante da união**. *Dado um código esférico $\mathcal{C} \subset S^{n-1}$ com M pontos e distância mínima $d = 2\text{sen}\left(\frac{\theta}{2}\right)$, vale a desigualdade*

$$M \leq \frac{A(C(n,\pi))}{A\left(C\left(n,\frac{\theta}{2}\right)\right)} = \frac{a_n}{a_{n-1}\int_0^{\frac{\theta}{2}} \text{sen}^{n-2}(\alpha)d\alpha}. \tag{2.26}$$

Analogamente, podemos escrever o limitante de Gilbert-Varshamov (2.21) como

$$M \geq \frac{A(C(n,\pi))}{A\left(C\left(n,\theta\right)\right)} = \frac{a_n}{a_{n-1}\int_0^{\theta} \text{sen}^{n-2}(\alpha)d\alpha}. \quad \square \tag{2.27}$$

2.4 Estimativas de Volume de Bishop-Gunther

Fica claro pelo exposto na seção anterior que para obtermos os limitantes no tamanho dos códigos, fixada uma distância mínima, é necessário o cálculo do volume de bolas na variedade $\mathcal{M}$. Em geral, isto é uma tarefa bastante difícil mesmo em exemplos mais simples. Alternativamente, uma ferramenta comum para o cálculo de volumes usada em geometria riemanniana surge a partir da curvatura, utilizando campos de Jacobi [14]. Os resultados não apresentam fórmulas exatas, mas sim estimativas para o volume baseadas em hipóteses na curvatura da variedade. Esta seção é dedicada a uma breve descrição desta técnica, de fundamental importância em nosso estudo.

Dado um ponto $x \in \mathcal{M}$, considere $\gamma : [0, +\infty) \longrightarrow \mathcal{M}$ uma geodésica normalizada, tal que $\gamma(0) = x$. Se $t > 0$ é pequeno suficiente, sabemos que $\gamma([0, t])$ é um caminho que minimiza a distância. Além disso, o conjunto dos pontos $t > 0$ com esta propriedade é um intervalo da forma $[0, t_0]$ ou $[0, +\infty)$. No primeiro caso, o ponto $\gamma(t_0)$ é dito um *ponto mínimo* de x em $\mathcal{M}$ sobre γ, e no segundo caso, dizemos que este ponto não existe.

Definição 2.4.1 *Definimos o* **cut-locus** $c(x)$ *como a união de todos os pontos mínimos de* $x \in \mathcal{M}$*, sobre todas as geodésicas* γ*, tais que* $\gamma(0) = x$*.*

Por exemplo, se $\mathcal{M} = I\!R^n$ é um espaço euclidiano, então $c(x) = \emptyset$ para todo $x \in \mathcal{M}$. Se $\mathcal{M} = S^2$ é a esfera unitária, então $c(x) = \{-x\}$ é o ponto antipodal, para todo $x \in \mathcal{M}$.

Denotamos o volume da bola geodésica de raio $\rho > 0$, numa variedade de curvatura constante $a \in I\!R$, por $V^a(\rho)$. Lembramos que ([9], cap. 13) se $(\mathcal{M}, \lambda)$ tem curvatura constante $a \in I\!R$ então:

- Se $a = 0$ então $\mathcal{M} = I\!R^n$ é um espaço Euclidiano;
- Se $a > 0$ então $\mathcal{M} = S^n$ é uma esfera;
- Se $a < 0$ então $\mathcal{M} = H^n$ é um espaço hiperbólico.

Podemos assumir, sem perda de generalidade, que $a = 0$, 1 ou -1.

Para qualquer variedade Riemanniana $(\mathcal{M}^d, \lambda)$, sua curvatura de Ricci é definida como a soma

$$\mathrm{Ric}(e_i) = \sum_{j=1}^{d} K(e_i, e_j), \tag{2.28}$$

onde $\{e_i\}$ é uma base ortonormal do espaço tangente de $\mathcal{M}$. É importante observar que (2.28) não depende da escolha da base [9]. O próximo teorema fornece limitantes para o volume de uma bola geodésica numa variedade riemanniana qualquer a partir de hipóteses sobre sua curvatura.

Teorema 2.4.1 (Bishop-Gunther [14]) *Sejam $(\mathcal{M}, \lambda)$ uma variedade Riemanniana completa de dimensão d, e $B_x(\rho)$ uma bola geodésica aberta em $\mathcal{M}$ que não intercepta o cut-locus de x.*

1. *Se existe uma constante α tal que* $\mathrm{Ric} \geq (d-1)\alpha\lambda$, *então*

$$\nu(B_x(\rho)) \leq V^{\alpha}(\rho). \tag{2.29}$$

2. *Se existe uma constante β tal que $K \leq \beta$, então*

$$\nu(B_x(\rho)) \geq V^{\beta}(\rho). \tag{2.30}$$

Unindo as desigualdades do teorema acima, obtemos

$$V^{\beta}(\rho) \leq \nu(B_x(\rho)) \leq V^{\alpha}(\rho). \tag{2.31}$$

Esta nova desigualdade pode ser usada para estimar o volume de uma bola geodésica numa variedade de curvatura não constante, a partir do volume das bolas nas variedades de curvatura constante α e β.

Com o objetivo de encontrar tais constantes, suponhamos agora que $\{e_i\}_{i=1}^{d}$ é uma base ortonormal do espaço tangente em $x \in \mathcal{M}$. Então temos que

$$\mathrm{Ric}(e_i) \geq (d-1)\alpha\lambda(e_i, e_i) = (d-1)\alpha 1 \quad \Leftrightarrow \quad \alpha \leq \frac{\mathrm{Ric}(e_i)}{d-1},$$

e definimos

$$\underline{\kappa} := \frac{1}{d-1}\min_{i=1}^{d}\{\mathrm{Ric}(e_i)\}. \tag{2.32}$$

Então $\alpha = \underline{\kappa}$ será a constante que limita a curvatura inferiormente. Por outro lado, é claro que

$$\bar{\kappa} := \max\{K(X,Y) : \|X\| = \|Y\| = 1\} \tag{2.33}$$

pode sempre fazer o papel da constante superior β do teorema acima. Ou seja, $\bar{\kappa}$ é o valor máximo da curvatura seccional na esfera unitária do espaço tangente de $\mathcal{M}$.

Desse modo, um dos objetivos principais do trabalho será determinar as constantes $\underline{\kappa}$ e $\bar{\kappa}$ para variedades flag geométricas e grassmannianas complexas. Assim, será possível estimar o volume de bolas geodésicas, e então conseguir os limitantes.

Capítulo 3

Limitantes para Empacotamentos na Variedade Flag Geométrica

Neste capítulo apresentamos os resultados principais deste trabalho, descrevendo novos limitantes para o número de pontos e a distância mínima de empacotamentos de esferas em variedades flag geométricas [5]. Para tanto, é necessário um estudo preliminar das principais características e propriedades geométricas destas variedades. Isto é feito nas subseções 3.1.1 e 3.1.2, tendo em vista a descrição dos espaços homogêneos apresentada no capítulo anterior.

Posteriormente, em 3.1.3, calculamos a curvatura de Ricci e o valor máximo da curvatura seccional na esfera unitária do espaço tangente das variedades flag. Desse modo, podemos usar as estimativas de volume de Bishop-Ghunter para limitar o volume de uma bola geodésica, e assim, obter um limitante superior e um limitante inferior para o número de pontos de um código $\mathcal{C} \subset \mathcal{F}(n : n_1, ..., n_s)$, cuja distância mínima é conhecida. Além disso, um limitante superior para a distância mínima $\delta(\mathcal{C})$ é obtido através da desigualdade de Hamming [5].

Na seção 3.2 estes limitantes são calculados computacionalmente. Tabelas e gráficos com os resultados numéricos de algumas simulações são apresentados. Analisando tais resultados, é possível perceber uma perda de desempenho quando a dimensão do espaço cresce ou a distância mínima torna-se muito pequena.

Aplicando a mesma técnica geométrica com o intuito de estender os resultados de [5] para variedades flag generalizadas, encerramos este capítulo com um estudo da curvatura destas variedades. Neste caso, ao invés de adotar a representação matricial de vetores no espaço tangente, usamos a estrutura de álgebra de Lie subjacente e os resultados são expressos em função das constantes de estrutura da álgebra.

3.1 A Variedade Flag Geométrica

3.1.1 Definição e Propriedades Fundamentais

Seja G um grupo de Lie simples, compacto e conexo e considere S um *toro* (isto é, um subgrupo abeliano e compacto) de G. O espaço homogêneo

$$\mathcal{F} = \frac{G}{C(S)}, \tag{3.1}$$

onde $C(S)$ é o *centralizador* de S em G, é chamado **variedade flag generalizada** (ou Kähler C-space). Assim como os espaços simétricos, as variedades flag generalizadas são classificadas a partir da classificação de Cartan das álgebras de Lie semi-simples complexas [4].

Neste capítulo consideraremos apenas variedades flag do grupo especial unitário

$$SU(n) = \{A \in \mathbb{C}^{n\times n} : \overline{A}^t A = I_n \text{ e } \det(A) = 1\}, \tag{3.2}$$

cuja álgebra de Lie $\mathfrak{su}(n)$ corresponde à *forma real compacta* da álgebra especial linear $\mathfrak{sl}(n,\mathbb{C})$. Tais variedades podem ser definidas pelo quociente

$$\mathcal{F}(n : n_1, ..., n_s) = \frac{SU(n)}{S(U(n_1) \times ... \times U(n_s))}, \tag{3.3}$$

onde $n = \sum_{i=1}^{s} n_i$, e são denominadas **variedades flag geométricas**. Contudo, além da estrutura de espaço quociente dada por (3.3), $\mathcal{F}(n : n_1, ..., n_s)$ pode ser definida como o conjunto de todas as sequências $(\{0\} \subset V_1 \subset ... \subset V_{s-1} \subset \mathbb{C}^n)$ de subespaços

encaixados de $\mathbb{C}^n$ satisfazendo

$$n_i = \dim(V_i) - \dim(V_{i-1}), \tag{3.4}$$

para todo $i = 1, ..., s$; onde $V_0 = \{0\}$ e $V_s = \mathbb{C}^n$. Desse modo, (3.3) segue da ação transitiva

$$\Phi : SU(n) \times \mathcal{F}(n : n_1, ..., n_s) \longrightarrow \mathcal{F}(n : n_1, ..., n_s), \tag{3.5}$$

que leva $(V_1, ..., V_s)$ em $(AV_1, ..., AV_s)$, a seqüência dada pelas imagens de cada subespaço V_i pelo isomorfismo A. Observe que as variedades de Grassmann complexas

$$G_m(\mathbb{C}^{m+n}) = \frac{SU(m+n)}{S(U(m) \times U(n))} \tag{3.6}$$

são casos particulares de variedades flag geométricas dadas por $\mathcal{F}(m+n : m, n)$, para $m, n > 0$. Em particular, todo espaço projetivo complexo

$$P(\mathbb{C}^n) = \mathcal{F}(n+1 : 1, n) \tag{3.7}$$

também é uma variedade flag. Outro exemplo importante nessa classe são as chamadas *variedades flag maximais*

$$\mathcal{F}(n) = \frac{SU(n)}{S(U(1) \times ... \times U(1))}, \tag{3.8}$$

dadas por seqüências de subespaços encaixados de codimensão 1.

Dada uma variedade flag $\mathcal{F}(n : n_1, ..., n_s)$, considere

$$\mathfrak{su}(n) = \{X \in \mathbb{C}^{n \times n} : \overline{X}^t = -X \text{ e } \mathrm{tr}(X) = 0\} \tag{3.9}$$

a álgebra de Lie de $SU(n)$, e tome $\mathfrak{k} \subset \mathfrak{su}(n)$ a subálgebra definida por $\mathfrak{k} = \mathfrak{s}(\mathfrak{u}(n_1) \oplus ... \oplus \mathfrak{u}(n_s))$. Desse modo obtemos a decomposição usual

$$\mathfrak{su}(n) = \mathfrak{k} \oplus \mathfrak{m}, \tag{3.10}$$

onde $\mathfrak{m}$ é o complementar ortogonal de $\mathfrak{k}$ em $\mathfrak{su}(n)$ com respeito à forma de Cartan-Killing. O espaço tangente da variedade flag na origem $T_o\left[\mathcal{F}(n : n_1, ..., n_s)\right]$ pode então ser identificado com o subespaço $\mathfrak{m}$. Já observamos no capítulo anterior (proposição 1.1.3) a existência de uma correspondência biunívoca entre as métricas in-

variantes em $\mathcal{F}(n : n_1, ..., n_s)$ e os produtos internos Ad-invariantes em $\mathfrak{m}$ [6], [24]. A métrica invariante considerada aqui é a *métrica normal* g_N, cujo produto interno associado é simplesmente a restrição da forma de Cartan-Killing em $\mathfrak{m}$. Portanto, se $X, Y \in \mathfrak{m}$ então

$$g_N(X,Y) = -\frac{1}{2}\langle X, Y\rangle_{CK} = -\frac{1}{2}\mathrm{tr}(\overline{X}^t Y). \tag{3.11}$$

Segue que a norma de um vetor tangente $X \in \mathfrak{m}$ é dada por

$$\|X\|^2 = g_N(X,X) = \frac{1}{2}\|X\|_F^2, \tag{3.12}$$

onde $\|X\|_F = \left(\sum_{i,j=1}^{n} |x_{ij}|^2\right)^{\frac{1}{2}}$ denota *a norma de Frobenius* de matrizes. Observe que não existe perda de estrutura ao considerarmos $G_m(\mathbb{C}^{m+n})$ dada por (3.6) ao invés do quociente mais usual $U(m+n)/U(m)\times U(n)$, considerado em alguns outros trabalhos relacionado ao tema. De fato estes dois espaços são difeomorfos e isométricos.

Afim de descrever uma base ortonormal de $\mathfrak{m}$, considere para $1 \leq i, j \leq s$ as matrizes $n \times n$

$$\tilde{E}_{pq}^{ij},$$

que possuem entrada 1 na posição

$$(n_1 + ... + n_{i-1} + p, n_1 + ... + n_{j-1} + q),$$

e 0 (zero) nas demais entradas. Para $1 \leq i < j \leq s$ e $n_i \leq p, q \leq n_j$, definimos os vetores

$$A_{pq}^{ij} := (\tilde{E}_{pq}^{ij} - \tilde{E}_{qp}^{ji}) \tag{3.13}$$

e

$$S_{pq}^{ij} := \sqrt{-1}(\tilde{E}_{pq}^{ij} + \tilde{E}_{qp}^{ji}). \tag{3.14}$$

Lema 3.1.1 *[1] O conjunto*

$$\mathcal{B} = \{A_{pq}^{ij}, S_{pq}^{ij} : 1 \leq i < j \leq s \text{ e } n_i \leq p, q \leq n_j\}$$

é uma base ortonormal de $\mathfrak{m}$ *em relação à métrica normal.*

Segue por um cálculo direto que a dimensão de $\mathcal{F}(n : n_1, ..., n_s)$ como variedade diferenciável real é dada por

$$d = 2 \sum_{1 \leq i < j \leq s} n_i n_j. \tag{3.15}$$

Particularmente,

$$\dim \left[G_m(\mathbb{C}^{m+n}) \right] = 2mn \tag{3.16}$$

e

$$\dim \left[\mathcal{F}(n) \right] = n(n-1). \tag{3.17}$$

O volume total de $\mathcal{F}(n : n_1, ..., n_s)$ é obtido a partir do volume de $SU(n)$ e a caracterização homogênea dada em (3.3). Utilizando a fórmula

$$\text{vol}\left(S^{d-1}\right) = \frac{2\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}\right)}$$

para o cálculo do volume da esfera unitária $(d-1)$-dimensional em $\mathbb{R}^d$, e o difeomorfismo

$$S^{2n-1} \cong \frac{SU(n)}{SU(n-1)}, \ \forall n > 1;$$

obtemos a relação recursiva

$$\nu\left(SU(n)\right) = \frac{2\pi^n}{(n-1)!} \nu(SU(n-1)), \tag{3.18}$$

que implica que o volume total de $SU(n)$ é dado por

$$\nu(SU(n)) = \frac{1}{2\pi} \left(\prod_{i=1}^{n} \frac{2\pi^i}{(i-1)!} \right), \tag{3.19}$$

para todo $n > 1$. Desse modo, obtemos

$$\nu(\mathcal{F}(n : n_1, ..., n_s)) = \frac{\prod_{i=1}^{n} \frac{2\pi^i}{(i-1)!}}{\prod_{j=1}^{s} \left(\prod_{l=1}^{n_j} \frac{2\pi^l}{(l-1)!} \right)}. \tag{3.20}$$

Como conseqüência, o volume da variedade flag maximal e da variedade de Grass-

mann complexa são dados respectivamente por

$$\nu(\mathcal{F}(n)) = \frac{1}{(n-1)!}\prod_{i=1}^{n-1}\frac{\pi^i}{(i-1)!} \tag{3.21}$$

e

$$\nu\left(G_m(\mathbb{C}^{m+n})\right) = \frac{\prod_{i=n+1}^{m+n}\frac{2\pi^i}{(i-1)!}}{\prod_{j=1}^{m}\frac{2\pi^j}{(j-1)!}}. \tag{3.22}$$

3.1.2 Representação da Isotropia

Uma importante ferramenta no estudo das variedades flag é a *representação da isotropia*. Se G/K é uma variedade flag generalizada, a representação linear de álgebras de Lie

$$\rho : \mathfrak{k} \longrightarrow GL(\mathfrak{m}) \tag{3.23}$$

é chamada de representação da isotropia. Tal representação é completamente redutível [1], portanto podemos decompor o espaço tangente

$$\mathfrak{m} = \mathfrak{m}_1 \oplus ... \oplus \mathfrak{m}_l, \tag{3.24}$$

onde cada $\mathfrak{m}_i$ é uma componente irredutível de ρ. Particularmente, a representação da isotropia das variedades flag geométricas $\mathcal{F}(n : n_1, ..., n_s)$ possui uma boa descrição em termos de matrizes, que é apresentada a seguir.

Proposição 3.1.1 *[1] Para $\mathcal{F}(n : n_1, ..., n_s)$, as componentes irredutíveis da representação da isotropia são dadas por*

$$\mathfrak{m}_{ij} = \mathrm{span}_R\{A^{ij}_{pq}, S^{ij}_{pq} : n_i \leq p, q \leq n_j\}, \tag{3.25}$$

para todo $1 \leq i < j \leq s$. Desse modo, existem $\frac{s(s-1)}{2}$ componentes irredutíveis. Consequentemente, a variedade de Grassmann $G_m(\mathbb{C}^{m+n})$ é isotropicamente irredutível, ou seja, possui apenas uma componente $\mathfrak{m}_{12} = \mathfrak{m}$.

Exemplo 3.1.1 *Dada a variedade flag*

$$\mathcal{F}(8:3,2,2,1)=\frac{SU(8)}{S(U(3)\times U(2)\times U(2)\times U(1))},$$

as componentes irredutíveis da representação da isotropia de $\mathfrak{m}$ *são dadas pelos blocos nas matrizes da forma*

$$\begin{bmatrix} * & * & * & a_{11} & a_{12} & b_{11} & b_{12} & c_{11} \\ * & * & * & a_{21} & a_{22} & b_{21} & b_{22} & c_{21} \\ * & * & * & a_{31} & a_{32} & b_{31} & b_{32} & c_{31} \\ -\overline{a_{11}} & -\overline{a_{21}} & -\overline{a_{31}} & * & * & d_{11} & d_{12} & e_{11} \\ -\overline{a_{12}} & -\overline{a_{22}} & -\overline{a_{32}} & * & * & d_{21} & d_{22} & e_{21} \\ -\overline{b_{11}} & -\overline{b_{21}} & -\overline{b_{31}} & -\overline{d_{11}} & -\overline{d_{21}} & * & * & f_{11} \\ -\overline{b_{12}} & -\overline{b_{22}} & -\overline{b_{32}} & -\overline{d_{12}} & -\overline{d_{22}} & * & * & f_{21} \\ -\overline{c_{11}} & -\overline{c_{21}} & -\overline{c_{31}} & -\overline{e_{11}} & -\overline{e_{21}} & -\overline{f_{11}} & -\overline{f_{21}} & * \end{bmatrix}.$$

Por exemplo, $\mathfrak{m}_{13}$ *é o conjunto das matrizes*

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & b_{11} & b_{12} & 0 \\ 0 & 0 & 0 & 0 & 0 & b_{21} & b_{22} & 0 \\ 0 & 0 & 0 & 0 & 0 & b_{31} & b_{32} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -\overline{b_{11}} & -\overline{b_{21}} & -\overline{b_{31}} & 0 & 0 & 0 & 0 & 0 \\ -\overline{b_{12}} & -\overline{b_{22}} & -\overline{b_{32}} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

onde $b_{ij}\in\mathbb{C}$*, para todo* $i=1,2,3$ *e* $j=1,2$*.*

O próximo resultado nos fornece informação sobre o colchete de Lie entre as componentes irredutíveis da representação da isotropia de $\mathfrak{m}$. Esta informação será muito útil em nosso próximos cálculos.

Proposição 3.1.2 *[22] Considere a variedade flag* $\mathcal{F}(n:n_1,..,n_s)$ *e a decomposição usual* $\mathfrak{su}(n)=\mathfrak{k}\oplus\mathfrak{m}$*. Se* $\mathfrak{m}=\sum_{i<j}\mathfrak{m}_{ij}$ *é a decomposição em componentes irredutíveis da representação da isotropia, então valem as seguintes relações*

$$[\mathfrak{m}_{ij},\mathfrak{m}_{ij}]\subset\mathfrak{k}, \tag{3.26}$$

$$[\mathfrak{m}_{ij}, \mathfrak{m}_{rs}] \subset \mathfrak{m}, \text{ if } (i,j) \neq (r,s). \tag{3.27}$$

3.1.3 Cálculo da Curvatura

Como estamos considerando a métrica normal, a curvatura seccional de $\mathcal{F}(n : n_1, ..., n_s)$ possui a expressão (2.17)

$$K(X,Y) = \frac{1}{4}\|[X,Y]_{\mathfrak{m}}\|^2 + \|[X,Y]_{\mathfrak{k}}\|^2,$$

onde X e Y são vetores tangentes normalizados e o colchete de Lie é dado pelo produto comutador $[X,Y] = XY - YX$.

Lema 3.1.2 *[21] Denote por E_{ij} a matriz $n \times n$ com entrada 1 na posição (i,j) e 0 (zero) nas demais entradas. Então*

$$[E_{ij}, E_{kl}] = \delta_{jk}E_{il} - \delta_{il}E_{jk}. \tag{3.28}$$

Este lema será útil no cálculo do colchete entre vetores da base $\mathfrak{m}$. De fato, observe que as matrizes $\tilde{E}^{ij}_{pq}$ usadas para definir os vetores da base $\mathcal{B}$ são do tipo $E_{\alpha\beta}$, onde

$$\alpha = n_1 + ... + n_{i-1} + p$$

e

$$\beta = n_1 + ... + n_{j-1} + q.$$

Teorema 3.1.1 *[5] Considere a variedade flag geométrica $\mathcal{F}(n : n_1, ..., n_s)$ e tome X um vetor pertencente à base ortonormal $\mathcal{B}$, tal que $X \in \mathfrak{m}_{ij}$ para algum par (i,j) satisfazendo $1 \leq i < j \leq s$. Então*

$$\mathrm{Ric}(X) = n + (n_i + n_j). \tag{3.29}$$

Portanto, a curvatura de Ricci é constante em cada componente irredutível da representação da isotropia.

Demonstração: A partir da definição da curvatura de Ricci (2.28) e também observando a fórmula (2.17) para a curvatura seccional, para provar o teorema precisamos

calcular a norma do colchete de Lie entre os vetores da base $\mathcal{B} = \{A_{pq}^{ij}, S_{pq}^{ij}\}$. Considerando

$$A_{\alpha\beta} = E_{\alpha\beta} - E_{\beta\alpha},\ S_{\alpha\beta} = \sqrt{-1}(E_{\alpha\beta} + E_{\beta\alpha}),$$

$$A_{\gamma\eta} = E_{\gamma\eta} - E_{\eta\gamma} \text{ and } S_{\gamma\eta} = \sqrt{-1}(E_{\gamma\eta} + E_{\eta\gamma}),$$

com $1 \leq \alpha < \beta \leq n$ e $1 \leq \gamma < \eta \leq n$, segue por um cálculo direto usando (3.28) que

$$\|[A_{\alpha\beta}, A_{\gamma\eta}]\|^2 = \delta_{\beta\gamma} + \delta_{\alpha\eta} + \delta_{\alpha\gamma} + \delta_{\beta\eta}. \tag{3.30}$$

De modo similar, $\|[S_{\alpha\beta}, S_{\gamma\eta}]\|^2$ e $\|[A_{\alpha\beta}, S_{\gamma\eta}]\|^2$ são iguais a (3.30). Finalmente, calculamos

$$\|[A_{\alpha\beta}, S_{\alpha\beta}]\|^2 = 4. \tag{3.31}$$

Portanto, se $(\alpha, \beta) \neq (\gamma, \eta)$ então

$$\|[A_{\alpha\beta}, A_{\gamma\eta}]\|^2 = \|[S_{\alpha\beta}, S_{\gamma\eta}]\|^2 = \|[A_{\alpha\beta}, S_{\gamma\eta}]\|^2 = 1.$$

Fixamos um vetor da base $\mathcal{B}$, por exemplo

$$A_{\alpha\beta} = A_{pq}^{ij} \in \mathfrak{m}_{ij},\ \text{para } (p < q,\ i < j).$$

Usando a representação matricial dos vetores tangentes e as fórmulas (3.30)-(3.31), vemos que a curvatura seccional é não nula nos vetores que constituem as linhas α, β e as colunas α, β. A curvatura de Ricci na direção de $A_{\alpha\beta}$ será determinada contando-se esses elementos, observando-se as relações da proposição 2.1.2. Obtemos assim:

- parte $\mathfrak{m}$, isto é, não considerando os vetores $\mathfrak{m}_{ij}$:

$$4\left(\sum_{t=1}^{i-1} n_t + \sum_{t=i+1}^{j-1} n_t + \sum_{t=j+1}^{s} n_t\right) = 4(n - (n_i + n_j)). \tag{3.32}$$

- parte $\mathfrak{k}$, isto é, considerando apenas vetores em $\mathfrak{m}_{ij}$:

$$2(n_i + n_j - 2) + 4, \tag{3.33}$$

  onde a última parcela da soma vem de (3.31).

Juntando (3.32) e (3.33), obtemos

$$\underbrace{4(n-(n_i+n_j))}_{\text{parte } \mathfrak{m}} + \underbrace{2(n_i+n_j-2)+4}_{\text{parte } \mathfrak{k}}, \tag{3.34}$$

e multiplicando pelos coeficientes presentes em (2.17), podemos concluir que

$$\mathrm{Ric}(A_{\alpha\beta}) = n + (n_i + n_j). \tag{3.35}$$

Segue que a curvatura de Ricci depende apenas da componente irredutível da representação da isotropia $\mathfrak{m}_{ij}$. ■

Corolário 3.1.1 *A variedade de Grassmann complexa $G_m(\mathbb{C}^{m+n})$ possui curvatura de Ricci constante*

$$\mathrm{Ric}(X) = 2(m+n), \tag{3.36}$$

para todo vetor $X \in \mathcal{B}$.

Corolário 3.1.2 *A variedade flag maximal $\mathcal{F}(n)$ possui curvatura de Ricci constante*

$$\mathrm{Ric}(X) = n+2, \tag{3.37}$$

para todo vetor $X \in \mathcal{B}$.

3.2 Limitantes para $|\mathcal{C}|$ e $\delta(\mathcal{C})$

3.2.1 Descrição dos Limitantes

Seguindo a técnica apresentada em [18], procedemos a seguir afim de derivar limitantes para empacotamentos de esferas na variedade flag geométrica. Para tanto, primeiramente é preciso calcular os limitantes $\underline{\kappa}$ (2.32) e $\overline{\kappa}$ (2.33) para a curvatura de $\mathcal{F}(n : n_1, ..., n_s)$. O próximo teorema é uma conseqüência imediata dos resultados anteriores sobre a curvatura de Ricci.

Teorema 3.2.1 *Para a variedade flag geométrica $\mathcal{F}(n : n_1, ..., n_s)$ obtemos a expressão explícita*

$$\underline{\kappa} = \frac{1}{d-1}\min_{1\leq i<j\leq s}\{n + (n_i + n_j)\}, \tag{3.38}$$

onde d é a dimensão de $\mathcal{F}(n : n_1, ..., n_s)$ dada em (3.15).

Em decorrência do teorema acima, obtemos o valor

$$\underline{\kappa} = \frac{m+n}{2mn-1}, \tag{3.39}$$

para a variedade Grassmann $G_m(\mathbb{C}^{m+n})$. Ainda, para a variedade flag maximal $\mathcal{F}(n : 1, ..., 1)$ resulta

$$\underline{\kappa} = \frac{n+2}{n^2-n-1}. \tag{3.40}$$

Tome $X, Y \in \mathfrak{m}$ dois vetores tangentes unitários. Sabendo que

$$[X, Y] = [X, Y]_{\mathfrak{k}} + [X, Y]_{\mathfrak{m}}$$

é uma soma de componentes ortogonais, segue que

$$K(X, Y) = \frac{1}{4}\|[X, Y]\|^2 + \frac{3}{4}\|[X, Y]_{\mathfrak{k}}\|^2 \leq$$

$$\leq \|[X, Y]\|^2 = \|XY - YX\|^2 \leq (2\|X\|\|Y\|)^2$$

$$\Rightarrow \quad K(X, Y) \leq 2^2 = 4.$$

Além disso, vimos na demonstração do teorema anterior que existem vetores unitários em $\mathcal{B} \subset \mathfrak{m}$ tais que o quadrado da norma de seu colchete é igual a 4. Desse modo, obtemos o seguinte resultado.

Proposição 3.2.1 *Para toda variedade flag geométrica $\mathcal{F}(n : n_1, ..., n_s)$, o valor máximo da curvatura seccional na esfera unitária do espaço tangente $\mathfrak{m}$ é*

$$\overline{\kappa} = 4. \tag{3.41}$$

Os resultados acima aprimoram o valor $\underline{\kappa} = 0$ considerado em [18] afim de obter limitantes para empacotamentos em $G_m(\mathbb{C}^{m+n})$. Por outro lado, observamos que

$\overline{\kappa} = 4$, o limitante superior para a curvatura seccional de $G_m(\mathbb{C}^{m+n})$ considerado em [18], também é válido para toda variedade flag geométrica $\mathcal{F}(n : n_1, .., n_s)$. Isto torna possível obter novos limitantes para empacotamentos em variedades flag, e consequentemente, também para Grassmannianas.

Afim de enunciar nossos próximos resultados, considere $S^{d-1}(r)$ a esfera Euclidiana de raio $r > 0$ em $\mathbb{R}^d$. Dado qualquer ponto $X \in S^{d-1}(r)$, denotaremos por $C_r(d, X, \phi)$ o *chapéu esférico* centrado em X de raio geodésico dado pelo ângulo de separação $0 \leq \phi \leq \pi$ [12]. A área $(d-1)$-dimensional de $C_r(d, X, \phi)$ não depende de seu centro, e será denotada por $V_r(d, \phi)$. Fixados uma dimensão d e um raio $r > 0$, a aplicação $\phi \longmapsto V_r(d, \phi)$ possui uma inversa monotônica

$$(V_r)^{-1}(d, *) : \mathbb{R}_+ \longrightarrow \mathbb{R}_+. \tag{3.42}$$

Definição 3.2.1 *O* **raio de injetividade** *de uma variedade Riemanniana compacta $(\mathcal{M}, g)$ é definido por*

$$i(\mathcal{M}) = \inf_{p \in \mathcal{M}} \{d_g(p, c(p))\}, \tag{3.43}$$

onde $c(p)$ denota o cut-locus do ponto $p \in \mathcal{M}$.

O raio de injetividade de uma variedade está diretamente relacionado à invertibilidade de sua aplicação exponencial. De fato, se $0 < r \leq i(\mathcal{M})$ então

$$\exp_p : T_p(\mathcal{M}) \longrightarrow \mathcal{M}$$

é bijetora na bola aberta $B_p(r) \subset \mathcal{M}$, para todo $p \in \mathcal{M}$. Este fato permite a construção de códigos em $\mathcal{M}$ por meio da aplicação exponencial, como feito em [23] para Grassmannianas. Portanto, um conjunto finito de vetores no espaço tangente pode ser mapeado em um código sobre a variedade, de modo que a função de codificação (ie. $\exp_p$) é inversível.

Feitas estas considerações, estamos prontos para enunciar e demonstrar um resultado central neste trabalho. O próximo teorema fornece um limitante inferior e um limitante superior para o número de pontos de um código em uma variedade flag geométrica, desde que seja conhecida sua distância mínima.

Teorema 3.2.2 *Considere a variedade flag geométrica $(\mathcal{F} = \mathcal{F}(n : n_1, ..., n_s)^d, g_N)$ e tome $0 < \rho_0 < i(\mathcal{F})$. Então existe um código $\mathcal{C} \subset \mathcal{F}$, com distância mínima maior ou igual a ρ_0, satisfazendo*

$$\frac{\nu(\mathcal{F})}{V_a(d, \rho_0)} := L \leq |\mathcal{C}|, \tag{3.44}$$

onde

$$a = \sqrt{\frac{d-1}{\min_{1\leq i<j\leq s}\{n + (n_i + n_j)\}}}.$$

Além disso, para todo código $\mathcal{C} \subset \mathcal{F}$ com distância mínima ρ_0, vale

$$|\mathcal{C}| \leq U := \frac{\nu(\mathcal{F})}{V_b\left(d, \frac{\rho_0}{2}\right)}, \tag{3.45}$$

onde $b = \frac{1}{2}$.

Demonstração: Usando as estimativas de volume de Bishop-Gunther [14] (teorema 3.101), com dados para a curvatura $\underline{\kappa}$ e $\bar{\kappa}$ obtidos em (3.38) e (3.41), obtemos

$$\nu^{\underline{\kappa}}(\rho_0) \geq \nu\left(B_{\delta_g}(\rho_0)\right)$$

e

$$\nu^{\bar{\kappa}}\left(\frac{\rho_0}{2}\right) \leq \nu\left(B_{\delta_g}\left(\frac{\rho_0}{2}\right)\right),$$

onde $\nu^{\underline{\kappa}}$ e $\nu^{\bar{\kappa}}$ denotam o volume de bolas geodésicas em variedades de curvatura constante $\underline{\kappa}, \bar{\kappa} \in I\!R$. Desse modo, através das desigualdades de Gilbert-Varshamov (2.21) e Hamming (2.22), segue que

$$\frac{\nu(\mathcal{M})}{\nu^{\underline{\kappa}}(\rho_0)} \leq |\mathcal{C}| \leq \frac{\nu(\mathcal{M})}{\nu^{\bar{\kappa}}\left(\frac{\rho_0}{2}\right)}.$$

Sabendo que $\underline{\kappa}$ e $\bar{\kappa}$ são números reais positivos, tais variedades são respectivamente as esferas Euclidianas $S^d(1/\sqrt{\underline{\kappa}})$ e $S^d(1/\sqrt{\bar{\kappa}})$, onde $d = \dim(\mathcal{F})$. Substituindo os valores obtidos em (3.38) e (3.41), segue o teorema. ■

Observamos a necessidade de requerer a condição $\rho_0 < i(\mathcal{F})$ como hipótese do teorema anterior, para assim podermos usar a estimativa de volume de Bishop-Gunther. De fato, em [14] (teorema 3.101) supõe-se que a bola aberta $B_p(\rho_0)$ na variedade $\mathcal{M}$ não intercepta o cut-locus of p. Este fato é sempre verdadeiro para todo $p \in \mathcal{M}$ assumindo-se que $\rho_0 < i(\mathcal{M})$, onde $i(\mathcal{M})$ denota o raio de injetividade de $\mathcal{M}$. Parti-

cularmente, toda variedade de Grassmann possui raio de injetividade igual a $\frac{\pi}{2}$ (veja, por exemplo, [33]). Portanto, como caso particular do teorema acima, obtemos o seguinte resultado para códigos em Grassmannianas.

Corolário 3.2.1 *Considere a variedade de Grassmann complexa* $(G = G_m(\mathbb{C}^{m+n}), g_N)$ *e tome* $0 < \rho_0 < \frac{\pi}{2}$. *Então existe um código* $\mathcal{C} \subset G_m(\mathbb{C}^{m+n})$, *com distância mínima maior ou igual* ρ_0, *satisfazendo*

$$\frac{\nu(G)}{V_a(2mn, \rho_0)} := L \leq |\mathcal{C}|, \tag{3.46}$$

onde

$$a = \sqrt{\frac{2mn-1}{m+n}}.$$

Além disso, para todo código $\mathcal{C} \subset G$ *com distância mínima* ρ_0, *vale*

$$|\mathcal{C}| \leq U := \frac{\nu(G)}{V_b\left(2mn, \frac{\rho_0}{2}\right)}, \tag{3.47}$$

onde $b = \frac{1}{2}$.

Os resultados acima garantem, para cada distância mínima fixada, a existência de um código na variedade flag geométrica cujo tamanho pode ser estimado por (3.44). Convém observar que, se a distância considerada for a que é conhecida como distância cordal (que está definida com detalhes na seção 4.2, eq. (4.14)), o volume normalizado de uma bola de raio $\rho < 1$ em $G_m(\mathbb{C}^{m+n})$ foi calculado de forma explícita em [11], e é dado por

$$\mu\left(B(\rho)\right) = c_{m,n}\rho^{2mn}, \quad \text{onde} \quad c_{m,n} = \frac{1}{mn!}\prod_{i=1}^{m}\frac{(m+n-i)!}{(m-i)!}. \tag{3.48}$$

Desse modo, usando a versão normalizada do limitante de Hamming $|\mathcal{C}|\mu\left(B\left(\frac{\delta}{2}\right)\right) \leq 1$ e (3.48), o limitante superior

$$|\mathcal{C}| \leq c_{m,n}^{-1}\left(\frac{\delta}{2}\right)^{-2mn} \tag{3.49}$$

foi apresentado em [26]. Além disso, como consequência de propriedades do mergulho esférico (4.20), o limitante (3.49) foi melhorado, obtendo-se o seguinte resultado.

Teorema 3.2.3 *[26] Para um código $\mathcal{C} \subset G_m(\mathbb{C}^{m+n})$ com distância mínima δ, com $m = 1$, $(m, n) = (2, 2)$, ou $\delta \leq \sqrt{4 - r^{-2}}$ com $r^2 = \frac{mn}{2(m+n)}$, vale*

$$|\mathcal{C}| \leq c_{m,n}^{-1} \left[2r^2 \left(1 - \sqrt{1 - \frac{\delta^2}{4r^2}} \right) \right]^{-mn}. \tag{3.50}$$

É importante notar que este resultado não melhora ou piora o limitante U de (3.46). De fato, estão sendo consideradas distâncias diferentes em $G_m(\mathbb{C}^{m+n})$ para obter cada resultado. Em (3.46), a distância em questão é a distância geodésica proveniente da métrica normal g_N, enquanto que em (3.50) considera-se a distância cordal, que é puramente topológica e não proveniente de métrica Riemanniana, mas sim do mergulho (4.20).

Considerando agora o problema dual, isto é, encontrar a distância mínima de um dado código $\mathcal{C} \subset \mathcal{M}$, é possível usar a desigualdade de Hamming para encontrar o seguinte limitante superior.

Teorema 3.2.4 *Para todo código $\mathcal{C} \subset \mathcal{F}(n : n_1, ..., n_s)$ com taxa binária $R(\mathcal{C})$, a distância mínima $\delta(\mathcal{C})$ deve satisfazer*

$$\delta(\mathcal{C}) \leq 2u, \tag{3.51}$$

onde $u = \left(V_{\frac{1}{2}}\right)^{-1} (d, \rho_0)$ e

$$\rho_0 = \frac{\nu(\mathcal{F}(n : n_1, ..., n_s))}{2^{dR(\mathcal{C})}}.$$

Observe que a fórmula (2.17) é válida não somente para variedades flag, mas também para todo espaço homogêneo G/H munido da métrica normal induzida por $\mathfrak{g}$. Portanto, o limitante u para a distância mínima de um empacotamento de esferas dado por (3.51) vale também nesse caso mais geral.

3.2.2 Cálculos Computacionais

A partir do desenvolvimento teórico da seção anterior, estamos prontos para calcular os limitantes estabelecidos em (3.44), (3.45) e (3.51). Observe que para encontrar L e U é suficiente calcular a área $(d-1)$-dimensional $V_r(d,\rho_0)$ de um chapéu esférico em $S^{d-1}(r) \subset I\!R^d$. Com este propósito, usaremos a expressão conhecida [12]:

$$V_r(d,\phi) = r^{d-1} a_{d-1} \int_0^{\phi} \text{sen}^{d-2}(t)dt, \tag{3.52}$$

onde

$$a_d = \begin{cases} \frac{(2\pi)^{d/2}}{(d-2)!!}, \text{ se } d = 2,4,6,... \\ \frac{2(2\pi)^{(d-1)/2}}{(d-2)!!}, \text{ se } d = 1,3,5,... \end{cases}.$$

Por outro lado, para encontrar o limitante superior u para a distância mínima $\delta(\mathcal{C})$, será necessário calcular a função inversa de $V_r(d,\phi)$. A saber, dado $v_0 > 0$ precisamos determinar o raio ϕ_0 tal que $V_r(d,\phi_0) = v_0$.

A Tabela-1 apresenta os resultados aproximados do cálculo dos limitantes $[L,U]$ para o número de pontos de códigos na variedade flag maximal $\mathcal{F}(n)$, para alguns valores $n \geq 2$ e distância mínima fixada $\rho_0 > 0$.

$n \backslash \rho_0$	0.25	0.5	1	1.5
2	$[128.67; 256.33]$	$[32.675; 64.334]$	$[8.7014; 16.337]$	$[4.3045; 7.454]$
3	$[51110.7; 1.0165 \times 10^8]$	$[898.07; 1.635 \times 10^6]$	$[22.478; 28738.4]$	$[4.321; 3069.54]$
4	$[2.34 \times 10^8; 6.92 \times 10^{16}]$	$[76788.4, 1.82 \times 10^{13}]$	$[61.882; 5.9714 \times 10^9]$	$[3.52; 1.7.55 \times 10^7]$
5	$[1.223 \times 10^{13}; 9.52 \times 10^{25}]$	$[2.007 \times 10^7; 1.392 \times 10^{23}]$	$[173.47; 2.284 \times 10^{17}]$	$[2.169; 1.7105 \times 10^{14}]$

Tabela 1. Limitantes $[L,U]$ para códigos em variedades flag maximais.

Primeiramente, observamos que estes cálculos foram realizados assumindo-se que o raio de injetividade de $\mathcal{F}(n)$ é maior ou igual que $\frac{\pi}{2}$. Para uma variedade flag qualquer, o valor explícito de $i(\mathcal{F})$ é por nós desconhecido. Contudo, acreditamos que $\frac{\pi}{2}$ é uma boa conjectura, pois este valor é válido para qualquer Grassmanniana e

também para $\mathcal{F}(3)$ [27]. De fato, o problema de encontrar o raio de injetividade é um tópico bastante relevante no estudo da geometria global das variedades flag, mas vai além do escopo deste trabalho, e portanto, não será discutido detalhadamente aqui.

Os resultados da tabela acima mostram claramente uma desempenho numérico fraco do limitante superior U, especialmente quando a dimensão de $\mathcal{F}(n)$ cresce (compare Fig. 3.1 e Fig. 3.2). De fato, os piores resultados aparecem para $\mathcal{F}(5)$, que é uma variedade diferenciável de dimensão 20. Contudo, obtemos alguns resultados satisfatórios para o limitante inferior L. Note ainda que, conforme a distância mínima cresce o limitante inferior L diminui, conforme é de se esperar. Ou seja, quanto maior o raio da bolas, menos espaço temos para arranjá-las. Para o maior valor da distância mínima $\rho_0 = 1.5$, o limitante inferior L é relativamente baixo; um indício de que este valor está próximo do raio de injetividade destas variedades.

As próximas figuras exibem os gráficos dos limitantes $[L, U]$ para empacotamentos de esferas no espaço projetivo complexo $\mathbb{C}P(2) = \mathcal{F}(2)$ e em $\mathcal{F}(3)$,respectivamente, com distância mínima variando entre $0.1 \leq \rho_0 \leq 1.5$. Observe que, ao passo que a distância mínima aproxima-se de zero, os limitantes assumem valores arbitrariamente grandes. Analisando a expressão (3.52) é possível ver que este fenômeno ocorre pois a área d-dimensional de um chapéu esférico aproxima-se rapidamente de zero quando seu raio decresce, enquanto que o volume total da variedade permanece constante. Por outro lado, os limitantes parecem tender a zero à medida que a distância mínima cresce. Com efeito, se o raio de uma bola geodésica em uma variedade compacta cresce, então existirá um ponto em que seu volume atingirá o volume total da variedade.

Em 1959, Shannon obteve o limitante inferior

$$1 - \frac{1}{2}\log_2(\rho_0(4 - \rho_0)) := L_S(\rho_0) \leq R(\rho_0) \tag{3.53}$$

para a taxa binária $R(\rho_0) = \limsup \left\{ \frac{\log_2(|\mathcal{C}|)}{n} \right\}$ de um código esférico $\mathcal{C} \subset S^{n-1}$, cuja distância Euclidiana mínima $\rho_0 > 0$ é dada [31]. Em outras palavras, se $M(n, \delta_0)$ denota o número máximo de pontos que podem ser colocados em S^{n-1} com distância

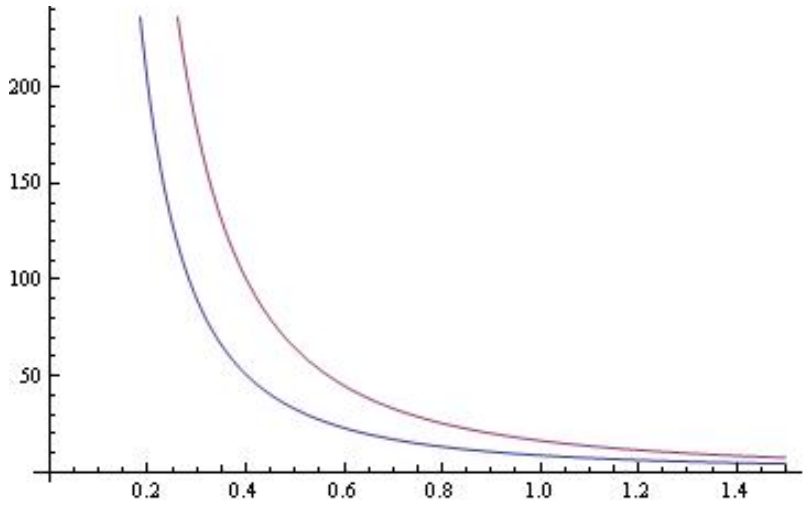

Figura 3.1: Limitantes $[L, U]$ para códigos $\mathcal{C} \subset \mathcal{F}(2)$, com $\rho_0 \in [0.1, 1.5]$

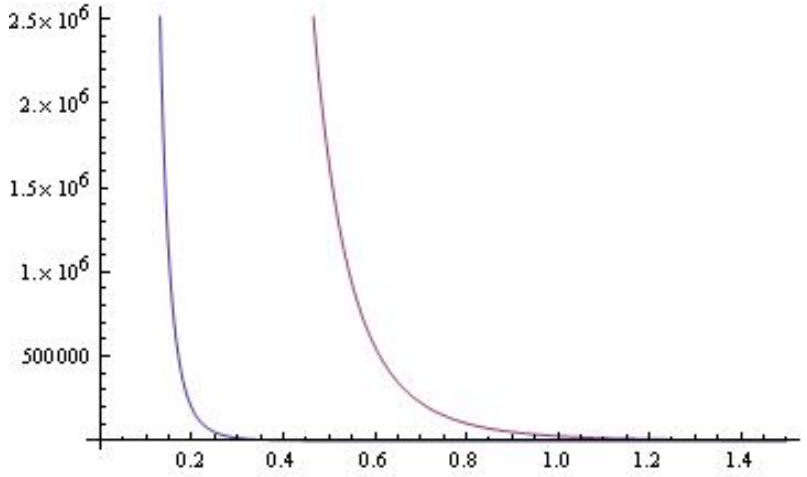

Figura 3.2: Limitantes $[L, U]$ para códigos $\mathcal{C} \subset \mathcal{F}(3)$, com $\rho_0 \in [0.1, 1.5]$

geodésica maior ou igual a $\theta_0 = 2\text{arcsen}(\rho_0/2)$, então

$$\frac{2^n}{[\rho_0(4-\rho_0)]^{\frac{n}{2}}} \leq M(n, \delta_0). \tag{3.54}$$

Afim de ilustrar o limitante inferior L dado em (3.44), considere

$$\mathcal{F}(3) = \frac{SU(3)}{S(U(1) \times U(1) \times U(1))},$$

a variedade flag maximal de $\mathbb{C}^3$, uma variedade diferenciável de dimensão real $d = 6$. Trata-se de um exemplo especial, pois é a primeira variedade flag que não é um espaço projetivo ou uma Grassmanniana complexa.

Usando (3.54), podemos observar que o tamanho de um código $\mathcal{C} \subset S^6$, com distância Euclidiana mínima $\rho_0 = 0.5$, deve satisfazer

$$11.94 \leq |\mathcal{C}|. \tag{3.55}$$

No entanto, o limitante L garante que é possível colocarmos ao menos 898 pontos $\mathcal{F}(3)$, cuja distância geodésica mínima é maior que $\rho_0 = 0.5$. Ou seja, $\mathcal{F}(3)$ é uma variedade compacta com a mesma dimensão de S^6, e para uma distância mínima fixada ρ_0, é possível colocarmos mais pontos em $\mathcal{F}(3)$ do que em S^6. O mesmo fenômeno ocorre com $G_1(\mathbb{C}^4)$, que também possui dimensão $d = 6$, e $L = 38.3179$ para $\rho_0 = 0.5$.

Nas tabelas 2, 3, 4 e 5 mostramos os valores aproximados dos limitantes $[L, U]$ para o tamanho de códigos em variedades de Grassmann $G_m(\mathbb{C}^{m+n})$, para alguns valores $m, n \geq 1$ e distâncias mínimas fixadas de 0.25, 0.5, 1 e 1.5, respectivamente.

$m\backslash n$	1	2	3	4
1	$[32.1672; 128.167]$	$[261.391; 32939.1]$	$[2180.72; 8.471 \times 10^6]$	$[18084.8; 2.18 \times 10^9]$
2	$[261.391; 32939.1]$	$[14815.1; 4.35807 \times 10^9]$	$[816285; 7.21162 \times 10^{14}]$	$[4.53 \times 10^7; 1.03 \times 10^{20}]$
3	$[2180.72; 8.471 \times 10^6]$	$[816285; 7.21162 \times 10^{14}]$	$[2.87697 \times 10^8; - - -]$	$[1.095 \times 10^{11}; 2.901 \times 10^{24}]$
4	$[18084.8; 2.18 \times 10^9]$	$[4.53 \times 10^7; 1.03 \times 10^{20}]$	$[1.09 \times 10^{11}; 2.901 \times 10^{24}]$	$[- - -; - - -]$

Tabela 2. Limitantes $[L, U]$ para códigos $\mathcal{C} \subset G_m(C^{m+n})$ com $\rho_0 = 0.25$.

$m\backslash n$	1	2	3	4
1	$[8.16877; 32.1672]$	$[17.3919; 2091.13]$	$[38.3179; 136295]$	$[84.1906; 8.89276 \times 10^6]$
2	$[17.3919; 2091.13]$	$[68.9689; 1.77855 \times 10^7]$	$[267.878; 1.89543 \times 10^{11}]$	$[1050.29; 2.26421 \times 10^{15}]$
3	$[38.3179; 136295]$	$[267.878; 1.89543 \times 10^{11}]$	$[1774.82; 4.43736 \times 10^{17}]$	$[11910.4; 1.45449 \times 10^{24}]$
4	$[84.1906; 8.89276 \times 10^6]$	$[1050.29; 2.26421 \times 10^{15}]$	$[11910.4; 1.45449 \times 10^{24}]$	$[135598; - - -]$

Tabela 3. Limitantes $[L, U]$ para códigos $\mathcal{C} \subset G_m(C^{m+n})$ com $\rho_0 = 0.5$.

$m\backslash n$	1	2	3	4
1	$[2.17534; 8.16877]$	$[1.39711; 139.135]$	$[0.95907; 2394.87]$	$[0.66592; 41398.6]$
2	$[1.3971; 139.135]$	$[0.54552; 82792.2]$	$[0.21587; 6.22018 \times 10^{7}]$	$[0.08737; 5.2515 \times 10^{10}]$
3	$[0.95907; 2394.87]$	$[0.21587; 6.22018 \times 10^{7}]$	$[0.04756; 2.7374 \times 10^{12}]$	$[0.01074; 1.58188 \times 10^{17}]$
4	$[0.66592; 41398.6]$	$[0.08737; 5.2515 \times 10^{10}]$	$[0.01074; 1.58188 \times 10^{17}]$	$[0.00134; 7.5254 \times 10^{23}]$

Tabela 4. Limitantes $[L, U]$ para códigos $\mathcal{C} \subset G_m(C^{m+n})$ com $\rho_0 = 1$.

$m\backslash n$	1	2	3	4
1	$[1.07612; 3.72702]$	$[0.41943; 30.51]$	$[0.18437; 255.795]$	$[0.08413; 2166.03]$
2	$[0.41943; 30.51]$	$[0.06892; 4332.05]$	$[0.01228; 787019]$	$[0.00231; 1.61471 \times 10^{8}]$
3	$[0.18437; 255.795]$	$[0.01228; 787019]$	$[0.000863; 4.15329 \times 10^{9}]$	$[0.0000643; 2.88986 \times 10^{13}]$
4	$[0.08413; 2166.03]$	$[0.00231; 1.61471 \times 10^{8}]$	$[0.0000643; 2.88986 \times 10^{13}]$	$[1.883 \times 10^{-6}; 8.19698 \times 10^{18}]$

Tabela 5. Limitantes $[L, U]$ para códigos $\mathcal{C} \subset G_m(C^{m+n})$ com $\rho_0 = 1.5$.

A simetria das tabelas anteriores se deve ao fato de que $G_m(\mathbb{C}^{m+n})$ e $G_n(\mathbb{C}^{m+n})$ serem a mesma variedade diferenciável. De fato, se $V \subset \mathbb{C}^{m+n}$ é um subespaço m-dimensional, então seu complementar ortogonal $V^{\perp}$ é únicamente determinado e pertence a $G_n(\mathbb{C}^{m+n})$. Desse modo, obtemos uma correspondência biunívoca $V \mapsto V^{\perp}$, que fornece um difeomorfismo entre estas variedades. Como no caso das flag maximais, observe que o limitante superior U perde eficiência com o crescimento da dimensão.

Considerando agora um empacotamento de esferas na variedade flag geométrica com taxa de informação dada por

$$R(\mathcal{C}) = \frac{\log_2|\mathcal{C}|}{d}, \tag{3.56}$$

(ou equivalentemente, $|\mathcal{C}| = 2^{dR(\mathcal{C})}$) podemos usar a função inversa (3.42) para calcular o limitante superior (3.51) em sua distância mínima $\delta(\mathcal{C})$.

A próxima tabela mostra os valores aproximados deste limitante para variedades de Grassmann complexas. Pelo mesmo motivo da Tabela-2, os dados apresentados estão simetricamente distribuídos. Os espaços tracejados ocorrem quando o software utilizado (*Wolfram - Mathematica*) não é capaz de alcançar o resultado devido à um

erro de aproximação grande. Erro este que parece ser ampliado com o crescimento na dimensão.

$m\backslash n$	1	2	3	4	5
1	1.0472	1.10817	1.14787	1.17679	1.19926
2	1.10817	1.35197	1.41825	1.47341	1.55164
3	1.14787	1.41825	1.61925	− − −	− − −
4	1.17679	1.47341	− − −	− − −	− − −
5	1.19926	1.55164	− − −	− − −	− − −

Tabela 6. Limitante $2u$ para códigos em $G_m(C^{m+n})$ com taxa $R(\mathcal{C}) = 1$.

$m\backslash n$	1	2	3	4	5
1	0.001953	0.001953	0.001953	0.001953	0.001953
2	0.001953	0.00213	0.0022335	0.0023034	0.0028486
3	0.001953	0.002335	0.0024039	0.006815	0.0161915
4	0.001953	0.0023034	0.006815	0.02008	0.0381902
5	0.001953	0.0028486	0.161915	0.0381902	0.0637021

Tabela 7. Limitante $2u$ para códigos em $G_m(C^{m+n})$ com taxa $R(\mathcal{C}) = 10$.

De fato, a técnica usada aqui para calcular a função inversa $\left(V_{\frac{1}{2}}\right)^{-1}(d, \rho_0)$ é encontrar o zero da função

$$u(x) := V_{\frac{1}{2}}(d, x) - \rho_0, \quad x \in [0, \pi]. \tag{3.57}$$

Conforme mostramos nas próximas figuras, o crescimento da dimensão implica no decrescimento de $u(x)$. Portanto, $u(x)$ torna-se arbitrariamente próximo de zero para valores suficientemente grandes de d. As figuras 3.3 e 3.4 ilustram esse fenômeno.

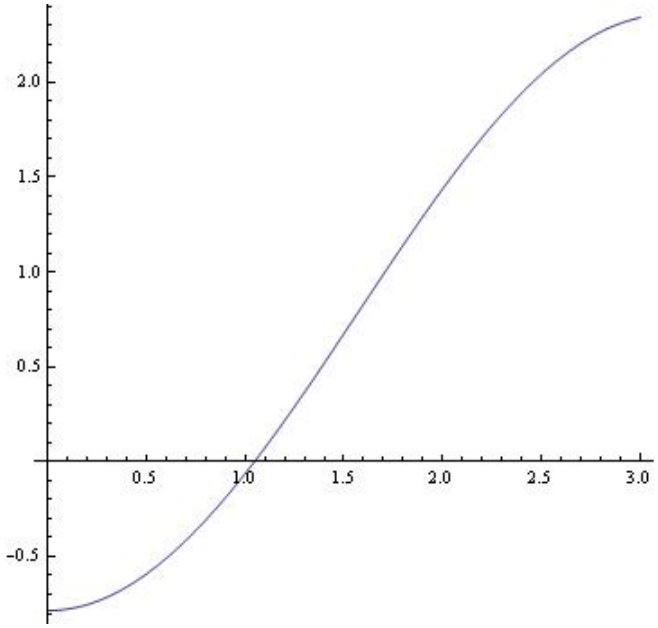

Figura 3.3: Gráfico de $u(x)$ para $\mathcal{M} = G_1(\mathbb{F}^2)$, $d = 2$.

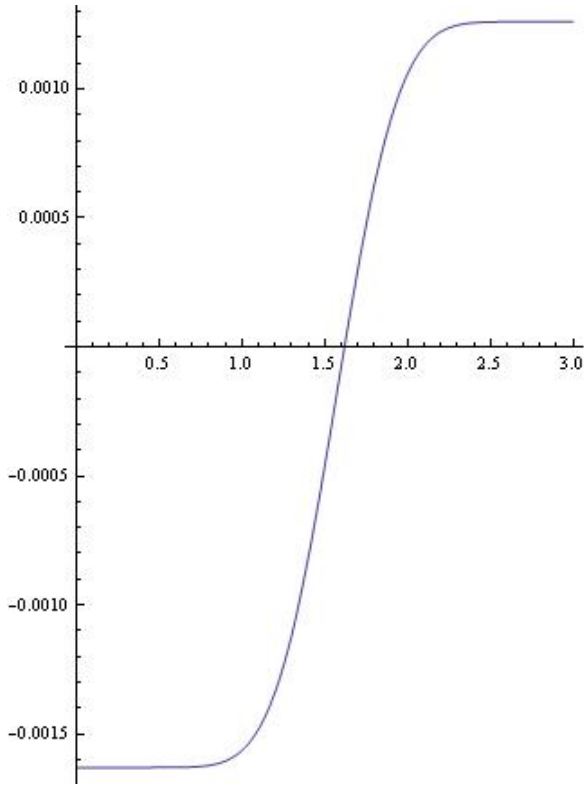

Figura 3.4: Gráfico de $u(x)$ para $\mathcal{M} = G_3(\mathbb{F}^5)$, $d = 12$.

Na figura 3.5 apresentamos o gráfico de $u(x)$ para $G_4(\mathbb{C}^7)$, que tem dimensão 24. Note que a curva é ainda mais "achatada", e a precisão do software não nos fornece o ponto de interseção dela com o eixo x. Isso se reflete em um dos espaços em branco da tabela 6.

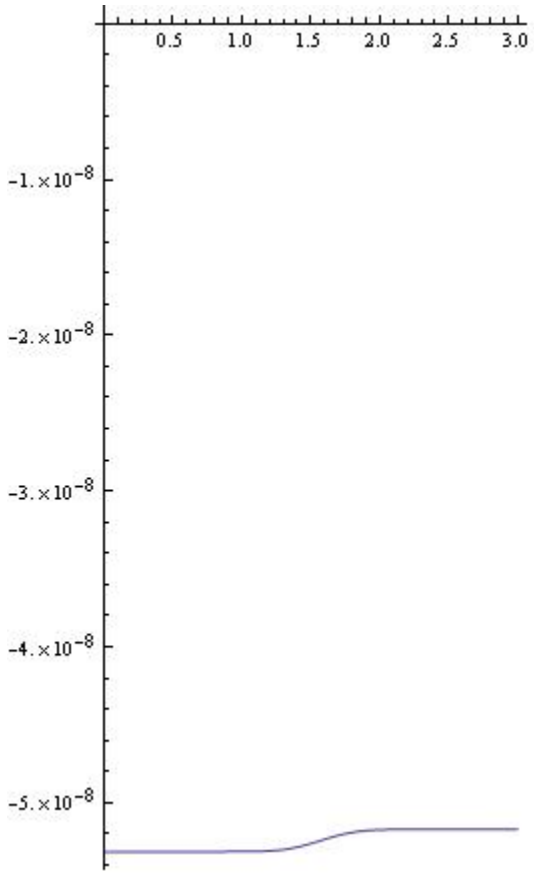

Figura 3.5: Gráfico de $u(x)$ para $\mathcal{M} = G_4(\mathbb{C}^7)$, $d = 24$.

Vale observarmos aqui que existe uma outra distância definida em $G_m(\mathbb{C}^{m+n})$ chamada *distância cordal* δ_c (4.14), que é topologicamente equivalente a distância geodésica δ_g pela relação

$$\delta_c \leq \delta_g \leq \frac{\pi}{2}\delta_c. \tag{3.58}$$

Em algumas situações, usar δ_c ao invés de δ_g é mais conveniente, e a desigualdade (3.58) garante que o limitante $2u$ em (3.51) também funciona para esta nova distância. Mais detalhes sobre a definição e as propriedades da distância cordal serão apresentados no próximo capítulo.

Finalmente, para as variedades flag maximais $\mathcal{F}(n)$, obtemos os seguintes resultados na distância mínima.

$n \backslash R(\mathcal{C})$	1	5	10	20
2	0.722734	0.00276214	2.69741×10^{-6}	4.70055×10^{-9}
3	0.810268	0.00295525	2.886×10^{-6}	4.5082×10^{-8}
4	0.0940055	0.00326714	0.0001427	0.0001427
5	1.09973	0.00504613	0.005056	0.005047
5	1.31533	0.0286204	0.02862	0.0286204

Tabela 8. Limitante $2u$ para códigos em $\mathcal{F}(n)$ com taxas $R(\mathcal{C}) \in \{0.5, 1, 5, 10\}$.

3.3 Empacotamentos em Variedades Flag Maximais

3.3.1 Definição da Variedade Flag Generalizada

Considere G um grupo de Lie complexo e simples com álgebra de Lie $\mathfrak{g}$. Seja $\mathfrak{h}$ uma subálgebra de Cartan de $\mathfrak{g}$, e denote por Π o conjunto de raízes associado ao par $(\mathfrak{g}, \mathfrak{h})$. Temos então a decomposição de $\mathfrak{g}$ em espaços de raízes

$$\mathfrak{g} = \mathfrak{h} \oplus \sum_{\alpha \in \Pi} \mathfrak{g}_\alpha, \tag{3.59}$$

onde $\mathfrak{g}_\alpha$ é um espaço de raiz (complexo e unidimensional) definido por

$$\mathfrak{g}_\alpha = \{X \in \mathfrak{g} : [H, X] = \alpha(H)X, \ \forall H \in \mathfrak{h}\}.$$

Seja $\Pi^+ \subseteq \Pi$ uma escolha de raízes positivas, e denote por Σ o correspondente sistema simples de raízes. Vamos fixar daqui em diante uma base de Weyl de $\mathfrak{g}$, isto é, um conjunto de vetores $X_\alpha \in \mathfrak{g}_\alpha$, $\alpha \in \Pi$ e $H_\alpha \in \mathfrak{h}$, $\alpha \in \Sigma$ satisfazendo

- $[X_\alpha, X_{-\alpha}] = H_\alpha$
- $[X_\alpha, X_\beta] = m_{\alpha,\beta} X_{\alpha+\beta}$, com $m_{\alpha,\beta}$ satisfazendo $m_{\alpha,\beta} = -m_{-\alpha,-\beta}$ e $m_{\alpha,\beta} = 0$ se $\alpha + \beta$ não é raiz.

Nesse ponto é importante observar que $m_{\alpha,\beta}$ é um número real. Mais detalhes sobre a existência da base de Weyl para álgebras de Lie simples podem ser encontrados em

[30] e [21].

Tome Θ um subconjunto qualquer de Σ, e seja $\langle\Theta\rangle$ o conjunto de raízes gerado por Θ. O conjunto $\Pi\backslash\langle\Theta\rangle$ será denotado $\langle\Theta\rangle^{\perp}$, e seus elementos serão chamados *raízes complementares* com respeito a Θ. Denotando $\langle\Theta\rangle^{+} = \langle\Theta\rangle \cap \Pi^{+}$, a decomposição (3.59) torna-se

$$\mathfrak{g} = \mathfrak{h} \oplus \sum_{\alpha\in\langle\Theta\rangle^{+}} \mathfrak{g}_{\alpha} \oplus \sum_{\alpha\in\langle\Theta\rangle^{+}} \mathfrak{g}_{-\alpha} \oplus \sum_{\beta\in\Pi^{+}\backslash\langle\Theta\rangle^{+}} \mathfrak{g}_{\beta} \oplus \sum_{\beta\in\Pi^{+}\backslash\langle\Theta\rangle^{+}} \mathfrak{g}_{-\beta}. \tag{3.60}$$

A *subálgebra parabólica* de $\mathfrak{g}$ determinada pela escolha Θ é

$$\mathfrak{p}_{\Theta} = \mathfrak{h} \oplus \sum_{\alpha\in\langle\Theta\rangle^{+}} \mathfrak{g}_{\alpha} \oplus \sum_{\alpha\in\langle\Theta\rangle^{+}} \mathfrak{g}_{-\alpha} \oplus \sum_{\beta\in\Pi^{+}\backslash\langle\Theta\rangle^{+}} \mathfrak{g}_{\beta},$$

e com essa notação, reescrevemos a equação (3.60) como

$$\mathfrak{g} = \mathfrak{p}_{\Theta} \oplus \sum_{\beta\in\Pi^{+}\backslash\langle\Theta\rangle^{+}} \mathfrak{g}_{-\beta}. \tag{3.61}$$

Definição 3.3.1 *Nas condições anteriores, a* **variedade flag generalizada** $\mathcal{F}_{\Theta}$*, associada ao par* $(\mathfrak{g}, \Theta)$*, é o espaço homogêneo*

$$\mathcal{F}_{\Theta} = \frac{G}{P_{\Theta}}, \tag{3.62}$$

onde P_{Θ} *é o normalizador de* $\mathfrak{p}_{\Theta}$ *em* G*.*

Tomamos uma forma real compacta de $\mathfrak{g}$, isto é, uma subálgebra real do tipo

$$\mathfrak{u} = \operatorname{span}_{R}\left\{\sqrt{-1}\mathfrak{h}_{R}, A_{\alpha}, S_{\alpha} : \alpha \in \Pi^{+}\right\}. \tag{3.63}$$

Os vetores geradores da álgebra $\mathfrak{u}$ são definidos por

$$A_{\alpha} = X_{\alpha} - X_{-\alpha} \quad \text{e} \quad S_{\alpha} = \sqrt{-1}(X_{\alpha} + X_{-\alpha}),$$

e $\mathfrak{h}_{R}$ é o espaço vetorial real gerado por $\{H_{\beta} : \beta \in \Sigma\}$. O conjunto

$$\mathcal{B} = \left\{A_{\alpha}, S_{\alpha}, \sqrt{-1}H_{\beta} : \alpha \in \Pi^{+} \text{ e } \beta \in \Sigma\right\} \tag{3.64}$$

é uma base ortogonal quando consideramos a forma de Cartan-Killing de $\mathfrak{g}$ restrita à $\mathfrak{u}$.

Considere $U = \exp_G(\mathfrak{u})$ a respectiva forma real compacta do grupo G. Denote $K_\Theta = U \cap P_\Theta$, e por construção, este é o centralizador de um toro. Então U age transitivamente em $\mathcal{F}_\Theta$, e podemos escrever

$$\mathcal{F}_\Theta = \frac{U}{K_\Theta}. \tag{3.65}$$

Desta caracterização, concluímos que a variedade flag é uma variedade diferenciável compacta. Quando $\Theta = \emptyset$, temos que $K_\Theta = T$ é o *toro maximal* de U, e obtemos a *variedade flag maximal*

$$\mathcal{F} = \frac{U}{T}. \tag{3.66}$$

As variedades flag geométricas tratadas no capítulo anterior são obtidas ao considerarmos a forma real compacta U como o grupo de matrizes

$$SU(n) = \{A \in \mathbb{C}^{n\times n} : \overline{A}^t A = I_n \text{ e } \det(A) = 1\},$$

e K_Θ como um subgrupo da forma $S(U(n_1) \times ... \times U(n_k))$, com $n_1 + ... + n_k = n$. A variedade maximal $\mathcal{F}(n)$ é obtida quando $n_i = 1$, para todo $i = 1, ..., n$; e consequentemente,

$$\mathcal{F}(n) = \frac{SU(n)}{T},$$

onde $T = S(U(1) \times ... \times U(1))$ é o toro maximal. Já vimos que esta variedade pode ser identificada com o conjunto formado pelos subespaços encaixados da forma $\{0\} = E_0 \subseteq E_1 \subseteq ... \subseteq E_n = \mathbb{C}^n$.

3.3.2 Curvatura em Flags Maximais

Na tentativa de estender nossos resultados para variedades flag mais gerais que as geométricas tratadas na seção 2.2, nos dedicamos agora ao cálculo da curvatura de Ricci de variedades flag maximais. De fato, para a obtenção dos valores $\underline{\kappa}$ e $\overline{\kappa}$, fundamentais para estabelecer os limitantes, é imprescindível um bom conhecimento da curvatura da variedade em questão. A estrutura de álgebra de Lie do espaço tangente é de grande importância no estudo da geometria das variedades flag. As expressões

para a curvatura seccional e a curvatura de Ricci são aqui obtidas em função das constantes de estrutura da álgebra de Lie associada. No exemplo 3.3.2 apresentamos o caso $\mathfrak{sl}(n,\mathbb{C})$, que trata-se justamente das variedades flag geométricas consideradas no capítulo anterior, e verificamos a compatibilidade com os resultados obtidos via a representação matricial do espaço tangente.

Os resultados apresentados aqui são frutos do trabalho conjunto com o Prof. Dr. Lino Anderson da Silva Grama do IMECC-Unicamp, cujas idéias e sugestões foram de grande valia durante o desenvolvimento da pesquisa realizada nesta tese. Salientamos ainda que este material encontra-se em desenvolvimento e não foi submetido para publicação, portanto, não há citações nem referência própria na bibliografia. De fato, encontrar os limitantes neste caso geral é uma tarefa mais difícil, pois a estrutura da álgebra de Lie associada pode ser bastante complexa. Contudo, do ponto de vista puramente geométrico, o cálculo da curvatura de uma variedade flag maximal é um resultado relevante, e será descrito a seguir.

Considere a variedade flag maximal $\mathcal{F} = \frac{U}{T}$, onde T é o toro maximal de U. Denote por $\mathfrak{t}$ a álgebra de Lie de T, e note que $\mathfrak{t}^C = \mathfrak{h}$. Seja $o = eT$ a origem de $\mathcal{F}$. O espaço tangente $T_o(\mathcal{F})$ pode ser identificado com o complementar ortogonal de $\mathfrak{t}$ em $\mathfrak{u}$ com respeito a forma de Cartan-Killing. Assim,

$$T_o(\mathcal{F}) := \mathfrak{m} = \text{span}_R\{A_\alpha, S_\alpha : \alpha \in \Pi^+\} = \sum_{\alpha\in\Pi^+} \mathfrak{u}_\alpha, \tag{3.67}$$

onde $\mathfrak{u}_\alpha = (\mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}) \cap \mathfrak{u}$. Dessa forma, temos

$$\mathfrak{u} = \mathfrak{t} \oplus \mathfrak{m}. \tag{3.68}$$

Complexificando $\mathfrak{m}$ obtemos o espaço tangente complexificado $T_o^C(\mathcal{F})$, que podemos identificar com

$$\mathfrak{m}^C = \sum_{\beta\in\Pi} \mathfrak{g}_\beta.$$

O próximo lema fornece o valor do colchete de Lie entre os elementos da forma real compacta de $\mathfrak{g}$.

Lema 3.3.1 *O colchete de Lie entre os elementos da base (3.64) de* $\mathfrak{u}$ *são dados pelas seguintes relações*

- $[\sqrt{-1}H_\alpha, A_\beta] = \beta(H_\alpha)S_\beta$;
- $[\sqrt{-1}H_\alpha, S_\beta] = -\beta(H_\alpha)A_\beta$;
- $[A_\alpha, S_\alpha] = 2\sqrt{-1}H_\alpha$;
- $[A_\alpha, A_\beta] = m_{\alpha,\beta}A_{\alpha+\beta} + m_{-\alpha,\beta}A_{\alpha-\beta}$;
- $[S_\alpha, S_\beta] = -m_{\alpha,\beta}A_{\alpha+\beta} - m_{\alpha,-\beta}A_{\alpha-\beta}$;
- $[A_\alpha, S_\beta] = m_{\alpha,\beta}S_{\alpha+\beta} + m_{\alpha,-\beta}S_{\alpha-\beta}$.

A forma de Cartan-Killing de $\mathfrak{g}$ restrita à $\mathfrak{u}$ é uma forma bilinear. Lembrando que a forma de Cartan-Killing é negativa definida, ao considerarmos o negativo desta forma bilinear teremos definido um produto interno em $\mathfrak{u}$, de modo que a norma dos vetores $\{A_\alpha,\ S_\alpha\}_{\alpha\in\Sigma}$ é igual a 2. A *métrica normal* em $\mathcal{F} = \frac{U}{T}$ será definida como a métrica Riemanniana correspondente à métrica bi-invariante de U induzida pelo produto interno

$$\langle X, Y\rangle = -\frac{1}{2}\langle X, Y\rangle_{CK} \tag{3.69}$$

em $\mathfrak{u}$. Observe que a multiplicação do fator $\frac{1}{2}$ torna a base (3.64) ortonormal.

Exemplo 3.3.1 (A álgebra de Lie $\mathfrak{sl}(n,\mathbb{C})$) *A álgebra especial linear $\mathfrak{g} = \mathfrak{sl}(n,\mathbb{C})$ é definida como o conjunto das matrizes complexas $n \times n$ de traço zero. Uma subálgebra de Cartan de $\mathfrak{g}$ é formada pelas matrizes diagonais*

$$\mathfrak{h} = \left\{ H = \operatorname{diag}(a_1, ..., a_n) : \sum_{i=1}^{n} a_i = 0 \right\}.$$

O sistema de raízes Π para o par $(\mathfrak{g}, \mathfrak{h})$ é dado por

$$\Pi = \{\alpha_{ij} := \varepsilon_i - \varepsilon_j : 1 \leq i \neq j \leq n\},$$

onde, para todo $1 \leq i \leq n$, ε_i é o funcional linear definido por

$$\varepsilon_i : D = \operatorname{diag}(a_1, ..., a_n) \longmapsto a_i \in \mathbb{C}.$$

O conjunto de raízes positivas é

$$\Pi^+ \{\alpha_{ij} := \varepsilon_i - \varepsilon_j : 1 \leq i < j \leq n\},$$

e o sistema simples de raízes

$$\Sigma = \left\{\alpha_{ij} \in \Pi^+ : j = i+1\right\}.$$

Os espaços de raízes são dados por $\mathfrak{g}_{\alpha_{ij}} = \mathrm{span}_C\{E_{ij}\}$*, onde* E_{ij} *é a matriz* $n \times n$ *com* 1 *na posição* ij *e zero nas demais posições. Observe que* $\alpha_{ij} = -\alpha_{ji}$*.*

Para determinar a forma real compacta de $\mathfrak{sl}(n,\mathbb{C})$*, definimos os vetores*

$$A_{\alpha_{ij}} = E_{ij} - E_{ji} \quad \text{e} \quad S_{\alpha_{ij}} = \sqrt{-1}(E_{ij} + E_{ji}),$$

onde $\alpha_{ij} \in \Pi^+$*. Note que estes vetores são precisamente aqueles que foram definidos anteriormente em (3.13) e (3.14). Tomando* $\mathfrak{u}_{\alpha_{ij}} = \mathrm{span}_R\left\{A_{\alpha_{ij}}, S_{\alpha_{ij}}\right\}$ *podemos decompor a álgebra real* $\mathfrak{u} = \mathfrak{su}(n)$ *como*

$$\mathfrak{u} = \sqrt{-1}\mathfrak{h} \oplus \sum_{\alpha_{ij}\in\Pi^+} \mathfrak{u}_{\alpha_{ij}}.$$

Note que $\mathfrak{u}_{\alpha_{ij}} = (\mathfrak{g}_{\alpha_{ij}} \oplus \mathfrak{g}_{\alpha_{ji}}) \cap \mathfrak{su}(n)$*. No caso particular* $\mathfrak{sl}(3,\mathbb{C})$*, dada a matriz*

$$A_{\alpha_{12}} = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

temos $A_{\alpha_{12}}\overline{A}^t_{\alpha_{12}} = \mathrm{diag}(1,1,0)$*, e portanto* $\|A_{\alpha_{12}}\|_F^2 := \mathrm{tr}(A_{\alpha_{12}}\overline{A}^t_{\alpha_{12}}) = 2$*, onde* $\|\ .\ \|_F$ *denota a norma de Frobenius de matrizes. Pode-se verificar que a norma induzida pela forma de Cartan-Killing em* $\mathfrak{su}(n)$ *é igual a metade da norma de Frobenius, considerando as matrizes em relação à base de Weyl.* □

A partir daqui, vamos fixar a métrica normal na variedade flag maximal, isto é, vamos considerar o par $\left(\mathcal{F} = \frac{U}{T}, g_N\right)$. Conforme observamos no capítulo 2, existe uma correspondência biunívoca entre métricas invariantes em $\mathcal{F}$ é produtos internos no espaço tangente $\mathfrak{m} = T_o(\mathcal{F})$ que são invariantes pela representação adjunta de T. Quando consideramos a métrica normal, o produto escalar é simplesmente a restrição do negativo da forma de Cartan-Killing ao subespaço $\mathfrak{m}$. Pelo corolário 1.1.1, sabemos que a curvatura de qualquer espaço homogêneo com a métrica normal é dada por

$$K(X,Y) = \frac{1}{4}\|[X,Y]_{\mathfrak{m}}\|^2 + \|[X,Y]_{\mathfrak{t}}\|^2.$$

Assim, usando as relações do lema 2.3.1 podemos calcular a curvatura entre os vetores da base (3.64). Temos

$$\begin{aligned} K(A_\alpha, A_\beta) &= \frac{1}{4}\|[A_\alpha, A_\beta]_{\mathfrak{m}}\|^2 + 0 \\ &= \frac{1}{4}\|m_{\alpha,\beta}A_{\alpha+\beta} + m_{-\alpha,\beta}A_{\alpha-\beta}\|^2 \\ &= \frac{1}{4}\langle m_{\alpha,\beta}A_{\alpha+\beta} + m_{-\alpha,\beta}A_{\alpha-\beta}, m_{\alpha,\beta}A_{\alpha+\beta} + m_{-\alpha,\beta}A_{\alpha-\beta}\rangle \\ &= \frac{1}{4}\left(m_{\alpha,\beta}^2\|A_{\alpha+\beta}\|^2 + m_{-\alpha,\beta}^2\|A_{\alpha-\beta}\|^2\right) \\ &= \frac{1}{4}\left(m_{\alpha,\beta}^2 + m_{-\alpha,\beta}^2\right). \end{aligned}$$

Por um cálculo análogo,

$$K(A_\alpha, S_\beta) = K(S_\alpha, S_\beta) = \frac{1}{4}\left(m_{\alpha,\beta}^2 + m_{\alpha,-\beta}^2\right),$$

e finalmente

$$\begin{aligned} K(A_\alpha, S_\alpha) &= 0 + \|[A_\alpha, S_\alpha]\|^2 \\ &= \|2\sqrt{-1}H_\alpha\|^2 \\ &= 4\|H_\alpha\|^2 = 4\langle H_\alpha, H_\alpha\rangle = 4\alpha(H_\alpha), \end{aligned}$$

onde $\alpha(H_\alpha)$ está relacionado com o comprimento da raiz α.

Fica claro que o cálculo da curvatura está intimamente ligado com a estrutura da álgebra de Lie do grupo. Ainda, estas fórmulas valem para qualquer flag maximal $\mathcal{F} = \frac{U}{T}$, desde que sejam conhecidas as constantes de estrutura $m_{\alpha,\beta}$ da álgebra de Lie em questão. Usando a fórmula $\mathrm{Ric}(e_i) = \sum_j K(e_i, e_j)$, onde $\{e_i\}$ é uma base ortonormal do espaço tangente, podemos calcular

$$\begin{aligned} \mathrm{Ric}(A_\alpha) &= \sum_{\beta\neq\alpha} K(A_\alpha, A_\beta) + \sum_{\beta\neq\alpha} K(A_\alpha, S_\beta) + K(A_\alpha, S_\alpha) \\ &= \frac{1}{4}\sum_{\beta\neq\alpha}\left(2m_{\alpha,\beta}^2 + m_{-\alpha,\beta}^2 + m_{\alpha,-\beta}^2\right) + \alpha(H_\alpha) \end{aligned}$$

e

$$\begin{aligned}
\mathrm{Ric}(S_\alpha) &= \sum_{\beta\neq\alpha} K(S_\alpha, S_\beta) + \sum_{\beta\neq\alpha} K(S_\alpha, A_\beta) + K(S_\alpha, A_\alpha) \\
&= \sum_{\beta\neq\alpha} K(S_\alpha, S_\beta) + \sum_{\beta\neq\alpha} K(A_\beta, S_\alpha) + K(A_\alpha, S_\alpha) \\
&= \frac{1}{4}\sum_{\beta\neq\alpha} \left(m^2_{\alpha,\beta} + m^2_{\alpha,-\beta} + m^2_{\beta,\alpha} + m^2_{\beta,-\alpha}\right) + \alpha(H_\alpha) \\
&= \frac{1}{4}\sum_{\beta\neq\alpha} \left(2m^2_{\alpha,\beta} + m^2_{-\alpha,\beta} + m^2_{\alpha,-\beta}\right) + \alpha(H_\alpha).
\end{aligned}$$

Obtemos assim o seguinte resultado.

Proposição 3.3.1 *A curvatura de Ricci de uma variedade flag maximal $\mathcal{F} = \frac{U}{T}$, munida da métrica normal, é dada por*

$$\mathrm{Ric}(A_\alpha) = \mathrm{Ric}(S_\alpha) = \frac{1}{4}\sum_{\beta\neq\alpha} \left(2m^2_{\alpha,\beta} + m^2_{-\alpha,\beta} + m^2_{\alpha,-\beta}\right) + \alpha(H_\alpha), \tag{3.70}$$

para quaisquer vetores da base $\{A_\alpha, S_\alpha : \alpha \in \Pi^+\}$.

Exemplo 3.3.2 *Considerando $\mathfrak{g} = \mathfrak{sl}(n,\mathbb{C})$, o resultado do corolário 2.1.2, que fornece a curvatura de Ricci de $\mathcal{F}(n)$, segue como conseqüência imediata dos cálculos anteriores. De fato, os vetores $\{X_\alpha : \alpha \in \Pi^+\}$ da base de Weyl que geram os espaços de raízes são neste caso os vetores $X_{\alpha_{ij}} = E_{ij}$ da base canônica de $\mathbb{C}^{n\times n}$, para $1 \leq i < j \leq n$. Usando (3.28) para calcular o colchete entre tais vetores quando $(i,j) \neq (k,l)$, obtemos*

- **a.** $j = k$ e $i \neq l \;\Rightarrow\; [E_{ij}, E_{kl}] = E_{il}$,
- **b.** $j \neq k$ e $i = l \;\Rightarrow\; [E_{ij}, E_{kl}] = -E_{jk}$,
- **c.** $j \neq k$ e $i \neq l \;\Rightarrow\; [E_{ij}, E_{kl}] = 0$.

Portanto, as constantes de estrutura da álgebra são $m_{ij} = \pm 1$ (casos a. e b.) ou $m_{ij} = 0$ (caso c.). Decorre que, fixado um par (i,j) com $1 \leq i < j \leq n$, o argumento da soma em (3.70) é não nulo apenas para (k,l) percorrendo a linha i ou a coluna j.

Segue então por uma contagem direta que

$$\begin{aligned}
\mathrm{Ric}(A_{\alpha_{ij}}) = \mathrm{Ric}(S_{\alpha_{ij}}) &= \frac{1}{4}\sum_{(k,l)\neq(i,j)}(2+1+1) + 4\|H_\alpha\|^2 \\
&= \frac{1}{4}4(n-2) + 4\frac{1}{2}\|H_\alpha\|_F^2 \\
&= (n-2)+4 \\
&= n+2. \ \square
\end{aligned}$$

Capítulo 4

Canais MIMO e a Variedade de Grassmann Complexa

Com o objetivo de apresentar uma perspectiva de aplicação dos limitantes obtidos na seção 2.2 no contexto da teoria de informação, abordaremos aqui a caracterização da capacidade de um canal de múltiplas antenas com desvanecimento. A expressão para a capacidade possui uma interpretação geométrica como um empacotamento na variedade de Grassmann complexa. Assim, códigos em grassmannianas, que a princípio são uma generalização natural dos códigos esféricos, também possuem aplicações na área de transmissão de sinais. Os detalhes do conteúdo apresentado na seção 3.1 podem ser encontrados em [8], [13], [20] e [35].

Na seção 3.2 apresentamos um estudo detalhado da distância geodésica e da distância cordal na variedade de Grassmann complexa. Para tanto, descrevemos o mergulho esférico de $G_m(\mathbb{C}^{m+n})$. Este mergulho permite que o *limitante de Rankin* para códigos esféricos também seja utilizado na obtenção de estimativas nestes novos espaços [8]. Encerramos o capítulo descrevendo o mergulho de uma variedade flag generalizada $\mathcal{F}$ numa grassmanniana através da representação adjunta do grupo de Lie associado, que juntamente com o mergulho esférico, fornece um mergulho de $\mathcal{F}$ numa esfera de raio e dimensão apropriados. Esta aplicação poderia ser utilizada para a generalização da distância cordal também para flags.

4.1 O Canal de Múltiplas Antenas

Um maior esforço tem sido feito no estudo de sistemas de comunicação sem fio (*wireless*) com uso múltiplas antenas, motivado pela necessidade de aumentar sua eficiência espectral [35]. Para um sistema de múltiplas antenas, com m antenas transmissoras e n antenas receptoras, e *desvanecimento Rayleigh* independente e identicamente distribuído (*i.i.d.*) entre todos os pares de antenas, o ganho de capacidade é $\min\{m, n\}$ bits por segundo por hertz para todo crescimento de 3-dB SNR [13]. Este resultado é derivado da hipótese de que os coeficientes de desvanecimento instantâneos são conhecidos pelo receptor. Portanto, esse resultado pode ser visto como um limite fundamental para comunicações de múltiplas antenas no caso *coerente*. Contudo, em ambientes móveis de comunicação sem fio, os coeficientes de desvanecimento podem variar muito rapidamente e as estimativas dos parâmetros do canal tornam-se difíceis, particularmente em sistemas com um grande número de antenas. Em tais situações, podemos estar interessados em explorar esquemas em que não sejam necessárias estimativas explícitas dos coeficientes de desvanecimento. Logo, existe interesse em entender os limites fundamentais para comunicações de múltiplas antenas no caso *não coerente*. Em [35], os autores usaram o mesmo modelo introduzido por Marzetta e Hochwald [20] para estudar a capacidade deste canal, para valores gerais de m e n, em um regime de alto SNR (*Signal-to-Noise Ratio*). Foi adotada uma abordagem geométrica, transformando o problema através de um novo sistema de coordenadas, cuja geometria subjacente é descrita mais naturalmente e o problema de otimização pode ser assim resolvido. Desse modo, obtém-se uma interpretação geométrica para a capacidade do canal como um empacotamento de esferas na variedade de Grassmann complexa. Descreveremos brevemente este estudo a seguir.

Assuma que o sistema de comunicação possua $m > 0$ antenas de transmissão e $n > 0$ antenas de recepção, com ruído Gaussiano independente e identicamente distribuído (i.i.d) em cada uma das antenas de recepção. Os coeficientes de propagação formam uma matriz $n \times m$ aleatória que ambos, transmissor e receptor, desconhecem. Adotaremos o modelo de desvanecimento Rayleigh. Também assumiremos que os coeficientes permanecem constantes por um período de tempo $t < \infty$, e que no próximo período mudam para uma nova configuração independente. A característica importante desse modelo é que o canal permanece constante apenas por um período finito de tempo, e então ocorre incerteza inerente ao canal no receptor. O número t

será denominado *tempo de coerência* do sistema. Devido à independência entre dois intervalos de coerência distintos, para calcularmos a capacidade deste canal é suficiente estudarmos apenas um intervalo de coerência, onde cada antena de transmissão envia um vetor complexo t-dimensional e cada antena de recepção também recebe um vetor do mesmo tipo.

Desse modo, sistema pode ser matematicamente descrito por

$$Y = HX + W, \tag{4.1}$$

onde $X \in \mathbb{C}^{m\times t}$ é a matriz cujo i-ésimo vetor linha $x_i \in \mathbb{C}^t$ corresponde ao sinal transmitido pela i-ésima antena, para todo $i = 1, ..., m$. Analogamente, $Y \in \mathbb{C}^{n\times t}$ e cada um de seus vetores linha $y_j \in \mathbb{C}^t$ corresponde ao sinal recebido pela j-ésima antena, para todo $j = 1, .., n$. A matriz $H \in \mathbb{C}^{n\times m}$ determina os ganhos de propagação h_{ij} da i-ésima antena de transmissão para a j-ésima antena de recepção, que são i.i.d. complexos Gaussianos $\mathbb{CN}(0, 1)$ distribuídos, com densidade

$$p(h_{ij}) = \frac{1}{\pi} e^{-|h_{ij}|^2}. \tag{4.2}$$

O ruído aditivo $W \in \mathbb{C}^{n\times t}$ possui entradas i.i.d. $w_{nl} \sim \mathbb{CN}(0, \sigma^2)$. Vamos normalizar a equação de modo que a potência média de transmissão em cada antena, no período de um símbolo, seja igual a 1. Então a restrição de potência pode ser escrita como

$$E\left[\sum_{i=1}^{m}\sum_{l=1}^{t} |x_{il}|^2\right] = mt. \tag{4.3}$$

Vamos nos referir ao SNR como a média dos SNR em cada antena de recepção. Pela normalização acima teremos $\text{SNR} = \frac{m}{\sigma^2}$.

A capacidade do canal (b/s/Hz) é definida como

$$C_{m,n}(\text{SNR}) = \frac{1}{t}\text{sup}_{p_x(.)}\{I(X;Y)\}, \tag{4.4}$$

onde $I(X;Y)$ denota a informação mútua e o índice subscrito indica o número de antenas disponível. A otimização é feita sobre todas distribuições de entrada de X satisfazendo a restrição de potência (4.3). Em [35], o objetivo dos autores foi calcular aproximações para $C_{m,n}(\text{SNR})$ com alto SNR, para vários valores de m, n e t. Tais

aproximações foram no sentido de que a diferença entre a aproximação e a capacidade $C_{m,n}(\text{SNR})$ tende a zero quando o SNR tende ao infinito. Para obter estas aproximações, o problema foi visto através de um novo sistema de coordenadas que será descrito a seguir.

Uma matriz X de tamanho $m \times t$, com $t \geq m$, pode ser representada como o subespaço $\Omega_X \subseteq \mathbb{C}^t$ gerado por seus vetores linha, juntamente a uma matriz C_X de tamanho $m \times m$, que especifica os vetores linha de X em relação a uma base canônica fixada em Ω_X. Assim, a transformação

$$X \longmapsto (C_X, \Omega_X) \tag{4.5}$$

fornece uma mudança de coordenadas $\mathbb{C}^{m\times t} \longrightarrow \mathbb{C}^{m\times m} \times G_m(\mathbb{C}^t)$. Observe que a dimensão do espaço de chegada $C^{m\times m} \times G_m(\mathbb{C}^t)$ é $2m^2 + 2m(t-m) = 2mt$, que é exatamente a dimensão real de $C^{m\times t}$. Seguindo esta idéia, é possível introduzir a aplicação

$$X \longmapsto (U_X, \Omega_1 \subset ... \subset \Omega_m \subset \mathbb{C}^t), \tag{4.6}$$

onde cada $\Omega_i = \text{span}_C\{x_1, ..., x_i\}$ é o subespaço gerado pelos primeiros i vetores linha de X, para $i = 1, ..., m$; e U_X é a matriz triangular superior que representa o processo de ortogonalização de Gram-Schmidt aplicado à base $\{x_1, ..., x_m\}$. Desse modo, obtemos uma nova mudança de coordenadas $\mathbb{C}^{m\times t} \longrightarrow U^{m\times m} \times \mathcal{F}(t : 1, ..., 1, t-m)$ envolvendo agora uma variedade flag geométrica, de modo que $\Omega_m = \Omega_X$. A dimensão do conjunto das matrizes triangulares superiores com entradas complexas $U^{m\times m}$ é $m(m+1) = m^2 + m$, enquanto que a dimensão da variedade flag em questão pode ser calculada usando a fórmula (3.15)

$$2\sum_{i<j} n_i n_j = 2\left[(m-1) + (t-m) + (m-2) + (t-m) + ... + (t-m)\right] =$$

$$= 2\left[m(t-m) + \sum_{k=1}^{m-1} k\right] = 2\left[mt - m^2 + \frac{m(m-1)}{2}\right] = 2mt - m^2 - m.$$

Portanto, a dimensão do espaço de chegada $U^{m\times m} \times \mathcal{F}(t : 1, ..., 1, t-m)$ é $(m^2 + m) + (2mt - m^2 - m) = 2mt$, que também coincide com a dimensão de $\mathbb{C}^{m\times t}$.

Para entendermos o efeito de (4.5), primeiro considere o canal sem o ruído aditivo: $Y = HX$. Neste caso, os vetores linha do sinal recebido Y geram o mesmo subespaço que os vetores linha do sinal enviado X, com probabilidade 1. Este fato mostra que os coeficientes aleatórios de desvanecimento afetam o sinal transmitido X mudando a matriz C_X, mas mantendo o subespaço Ω_X inalterado. Para o canal com o ruído aditivo (4.1), o subespaço Ω_X é corrompido apenas pelo ruído, mas a matriz C_X é corrompida por ambos, ruído e desvanecimento do canal. Essencialmente, o novo sistema de coordenadas decompõe $\mathbb{C}^{m\times t}$ em duas direções, uma afetada pelo ruído e desvanecimento, e outra afetada apenas pelo ruído. Em uma situação de alto SNR, a aleatoriedade de C_X é dominada pela aleatoriedade proveniente dos coeficientes de desvanecimento, em vez da proveniente do ruído aditivo. Intuitivamente, podemos pensar nesse caso que C_X é corrompida apenas pelo desvanecimento do canal. Portanto, o uso do sistema de coordenadas (4.5) nos permite considerar o efeito do desvanecimento e do ruído aditivo separadamente para uma situação de alto SNR.
O próximo teorema apresenta a expressão da capacidade do canal de múltiplas antenas no caso particular $m = n$ e $t \geq 2m$.

Teorema 4.1.1 *[35] Para o canal de múltiplas antenas (MIMO) com m antenas transmissoras, m antenas receptoras e tempo de coerência $t \geq 2m$, a capacidade para alto SNR (b/s/Hz) é dada por*

$$C_{m,m}(SNR) = m\left(1 - \frac{m}{t}\right)\log_2 SNR + c_{m,m} + o(1), \tag{4.7}$$

onde

$$c_{m,m} = \frac{1}{t}\log_2|G_m(\mathbb{C}^t)| + m\left(1 - \frac{m}{t}\right)\log_2\frac{t}{m\pi e} + \left(1 - \frac{m}{t}\right)E[\log_2\det(H\overline{H}^t)]$$

e

$$E[\log_2\det(H\overline{H}^t)] = \sum_{i=1}^{m} E[\log\chi^2_{2i}].$$

Vamos agora descrever a interpretação geométrica apresentada em [35], que relaciona o resultado sobre a capacidade destes sistemas com um empacotamento de esferas na Grassmanniana. Primeiramente, a informação mútua pode ser decomposta em duas parcelas

$$I(X;Y) = I(\Omega_X;Y) + I(C_X;Y|_{\Omega_X}), \tag{4.8}$$

através do novo sistema de coordenadas (4.5). Isto é, a informação mútua total é decomposta na informação mútua transmitida pelo subespaço Ω_X, e a informação

mútua transmitida dentro do subespaço. Como X é da forma $X = A\Theta$, onde Θ é uma matriz unitária independente de A, temos que $C_X = AQ$, onde Q é uma matriz $m \times m$ unitária independente de A. Consequentemente, podemos escrever $C_{HX} = HAQ$.

Vamos usar o fato de que a distribuição de entrada assintoticamente ótima para alto SNR é a entrada de norma constante igual

$$P(\|x_i\| = \sqrt{t}) = 1, \qquad \forall i = 1, ..., m.$$

Com isto, $C_X = \sqrt{t}Q$ e $C_{HX} = \sqrt{t}HQ$. Observe que H é por si só identicamente distribuída, e também que HQ é independente de Q. Portanto, Y é independente de $CX = \sqrt{t}Q$, isto é, a observação de Y não fornece informação sobre C_X. Concluímos que o segundo termo em (4.8) é zero, e assim toda a informação mútua é transmitida pelo subespaço aleatório Ω_X

$$I(X;Y) = I(\Omega_X;Y). \tag{4.9}$$

Desse modo, para um canal de múltiplas antenas não coerente, o objeto que transporta a informação é um subespaço aleatório Ω_X, que é um ponto qualquer na variedade de Grassmann.

A capacidade do canal *AWGN* canônico possui uma interpretação bem conhecida em termos de empacotamentos de esferas. Esta idéia pode ser generalizada para canais de múltiplas antenas, tanto no caso coerente como no não coerente. Para um canal não coerente, onde os coeficientes de desvanecimento são desconhecidos, podemos interpretar a capacidade como um empacotamento de esferas na variedade de Grassmann. Sabendo-se que o subespaço Ω_X é o objeto usado para transmitir informação, consideramos o sinal transmitido em cada intervalo de coerência como um ponto em $G_m(\mathbb{C}^t)$. Similarmente ao caso onde não há ruído, a matriz H altera o volume do espaço por um fator escalar, que resulta $\det\left(tH\overline{H}^t\right)^{t-m} \mathrm{vol}\left(G_m(\mathbb{C}^t)\right)$. Se o código tem palavras de comprimento $l > 0$, então o sinal recebido pertence à um espaço $\mathcal{M}$ produto de Grassmannianas, cuja dimensão é $d = lm(t-m)$. O ruído perturba o sinal na esfera $B_d\left(\sqrt{d\sigma^2}\right)$, e denotando $H_i,\ i = 1, ..., l$; como as matrizes dos coeficientes de desvanecimento no intervalo i, escrevemos a proporção dos dois

volumes

$$q := \frac{\mathrm{vol}(\mathcal{M})}{\mathrm{vol}\left(B_d(\sqrt{d\sigma^2})\right)} = \frac{\prod_{i=1}^{l} \det\left(tH\overline{H}^t\right)^{t-m} \mathrm{vol}\left(G_m(\mathbb{C}^t)\right)}{\mathrm{vol}\left(B_{lm(t-m)}(\sqrt{lm(t-m)\sigma^2})\right)},$$

e segue

$$\frac{1}{l}\log(q) = (t-m)\frac{1}{l}\sum_{i=1}^{l}\log\left(\det\left(tH_i\overline{H_i^t}\right)\right) + \log\left(\mathrm{vol}(G_m(\mathbb{C}^t))\right) -$$

$$-\frac{1}{l}\log\left(\mathrm{vol}\left(B_{lm(t-m)}(\sqrt{lm(t-m)\sigma^2})\right)\right).$$

Usando a fórmula $\mathrm{vol}(B_n(r)) = \pi^n r^{2n}/n!$ e a *fórmula de Stirling* $n! \approx n^n e^{-n}\sqrt{2\pi n}$, obtemos quando $n \longrightarrow \infty$

$$\begin{aligned}\frac{1}{n}\log\Big(\mathrm{vol}\big(B_n(r)\big)\Big) &= \frac{1}{n}\log\left(\frac{\pi^n r^{2n}}{n!}\right)\\ &\longrightarrow \frac{1}{n}\log\left(\frac{(\pi r^2)^n}{n^n e^{-n}\sqrt{2\pi n}}\right)\\ &\longrightarrow \log(\pi e r^2),\end{aligned}$$

portanto

$$\frac{1}{l}\log(q) - E\left[\log\left(\det\left(tH\overline{H}^t\right)\right)\right] + \log\left(\mathrm{vol}(G_m(\mathbb{C}^t))\right) - m(t-m)\log(\pi e\sigma^2) =$$

$$= m(t-m)\log SNR + c_{m,m}.$$

Esta expressão é justamente a capacidade dada em (4.7) pelo teorema anterior.

4.2 Distâncias na Grassmanniana e o Mergulho Esférico

A variedade de Grassmann complexa $G_m(\mathbb{C}^{m+n})$, ou simplesmente grassmanniana, é definida como o conjunto formado pelos subespaços m-dimensionais em $\mathbb{C}^{m+n}$, onde $m, n \geq 0$. Vimos na seção 2.1 que trata-se de um caso particular de variedade flag

geométrica. Uma descrição comum destas variedades usada em diversos textos é obtida a partir da *variedade de Stiefel*

$$V_m(\mathbb{C}^{m+n}) := \left\{ A \in \mathbb{C}^{(m+n)\times m} : \overline{A}^t A = I_m \right\}, \tag{4.10}$$

estabelecendo-se a relação de equivalência

$$A \simeq B \quad \Leftrightarrow \quad \exists\ P \in U(m) \ \text{ tal que } \ B = AP.$$

Ou seja, duas matrizes $A, B \in V_m(\mathbb{C}^{m+n})$ estão relacionadas se, e somente se, suas colunas geram o mesmo subespaço m-dimensional em $\mathbb{C}^{m+n}$. Desse modo

$$G_m(\mathbb{C}^{m+n}) = \frac{V_m(\mathbb{C}^{m+n})}{U(m)}. \tag{4.11}$$

Considerando em $\mathbb{C}^{m+n}$ o produto interno usual

$$u.v = \sum_{j=1}^{m+n} u_j \overline{v_j}, \tag{4.12}$$

podemos associar univocamente à cada subespaço $W \in G_m(\mathbb{C}^{m+n})$ seu complementar ortogonal $W^\perp$. Sabendo que $\dim\left(W^\perp\right) = (m+n) - m = n$, obtemos uma bijeção

$$\psi : G_m(\mathbb{C}^{m+n}) \longrightarrow G_n(\mathbb{C}^{m+n}).$$

Desse modo, podemos supor sem perda de generalidade que $0 \leq m \leq \frac{m+n}{2}$.

Com o objetivo de definir a distância entre dois pontos (isto é, m-planos) $X, Y \in G_m(\mathbb{C}^{m+n})$, definimos inicialmente *ângulos principais* $\theta_i \in [0, \frac{\pi}{2}]$ e *vetores principais* $u_i \in P$ e $v_i \in Q$, para $i = 1, ..., m$ [8]. Escolhemos dois vetores unitários $u_1 \in X$ e $v_1 \in Y$ de modo que o produto interno $u_1.v_1$ seja maximal (a compacidade da bola unitária e a continuidade do produto interno garantem a existência de tais vetores). Como a função arco-cosseno é decrescente em $[0, \pi]$, esta condição implica que o ângulo entre u_1 e v_1 é mínimo. Indutivamente, tomamos vetores unitários $u_i \in X$ e $v_i \in Y$ satisfazendo as condições

- $u_i.u_j = 0$ e $v_i.v_j = 0$, para todo $1 \leq j < i$;
- $u_i.v_i$ é maximal.

Então definimos $\theta_i = \arccos(u_i.v_i)$, para todo $i = 1, ..., m$, obtendo assim m ângulos principais $0 \leq \theta_1 \leq ... \leq \theta_m \leq \pi/2$.

A distância geodésica de $G_m(\mathbb{C}^{m+n})$, induzida pela métrica normal de $\mathfrak{su}(m+n)$, pode ser expressa através dos ângulos principais [33]

$$d_g(X,Y) = \sqrt{\sum_{i=1}^{m} \theta_i^2}. \tag{4.13}$$

Observamos que distância geodésica não é diferenciável em todo ponto. Por exemplo, considerando o caso $m = n = 1$, fixado um subespaço X (isto é, uma reta pela origem) enquanto giramos outro subespaço Y. Ao passo que o ângulo entre X e Y cresce de 0 a π, o ângulo principal θ_1 cresce de 0 a $\frac{\pi}{2}$ e então cai para 0, gerando a não diferenciabilidade. Uma definição alternativa de distância é dada a seguir.

Definição 4.2.1 *Dados dois pontos $X, Y \in G_m(\mathbb{C}^{m+n})$, a* **distância cordal** *entre eles é dada pela expressão*

$$d_c(P,Q) := \sqrt{\sum_{i=1}^{m} \text{sen}^2(\theta_i)}. \tag{4.14}$$

Sendo que $\theta_i \in [0, \frac{\pi}{2}]$, para todo $1 \leq i \leq m$, temos que $\text{sen}(\theta_i) \leq \theta_i$. Isto implica que

$$d_c(X,Y) \leq d_g(X,Y), \quad \forall X, Y \in G_m(\mathbb{C}^{m+n}).$$

Além disso, sabendo que $\lim_{\theta \to 0} \frac{\text{sen}(\theta)}{\theta} = 1$, podemos concluir que $d_c \to d_g$ quando os planos estão próximos. Observe ainda que $d_c(X,Y) \leq \sqrt{m}$. Por outro lado, usando que $\frac{\pi}{2}\text{sen}(\theta) \geq \theta$ em $[0, \frac{\pi}{2}]$, temos

$$\sum_{i=1}^{m} \theta_i^2 \leq \sum_{i=1}^{m} \left(\frac{\pi}{2}\text{sen}(\theta_i)\right)^2 = \frac{\pi^2}{4} \sum_{i=1}^{m} \text{sen}^2(\theta_i),$$

e consequentemente

$$d_g(X,Y) \leq \frac{\pi}{2} d_c(X,Y), \quad \forall X, Y \in G_m(\mathbb{C}^{m+n}).$$

Obtemos assim o seguinte resultado.

Proposição 4.2.1 *As distâncias d_g e d_c são topologicamente equivalentes em $G_m(\mathbb{C}^{m+n})$*

e obedecem à relação

$$d_c \leq d_g \leq \frac{\pi}{2} d_c \leq \frac{\pi\sqrt{m}}{2}. \tag{4.15}$$

Vamos agora descrever o mergulho esférico de $G_m(\mathbb{C}^{m+n})$ apresentado em [8]. Uma *matriz geradora* de um ponto $X \in G_m(\mathbb{C}^{m+n})$ é uma matriz complexa $(m+n) \times m$ cujas colunas geram X. A matriz geradora de um ponto não é única, e duas matrizes geradoras distintas são conjugadas por elementos de $U(m)$. A partir de uma escolha de bases conveniente, sempre é possível reduzir as matrizes geradoras de $X, Y \in G_m(\mathbb{C}^{m+n})$, respectivamente, às formas [33]

$$\left[\begin{array}{cccc} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & ... & 1 \\ \hline 0 & 0 & ... & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & ... & 0 \end{array}\right] \quad \text{e} \quad \left[\begin{array}{cccc} \cos(\theta_1) & 0 & ... & 0 \\ 0 & \cos(\theta_2) & ... & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & ... & \cos(\theta_m) \\ \hline \operatorname{sen}(\theta_1) & 0 & ... & 0 \\ 0 & \operatorname{sen}(\theta_2) & ... & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & ... & \operatorname{sen}(\theta_m) \\ \hline 0 & 0 & ... & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & ... & 0 \end{array}\right], \tag{4.16}$$

onde $\theta_i, 1 \leq i \leq m$, são os ângulos principais entre X e Y. Vamos associar a cada subespaço $W \in G_m(\mathbb{C}^{m+n})$ a projeção ortogonal $\Pi_W : \mathbb{C}^{m+n} \longrightarrow W$. Claramente essa relação é bijetora, e desse modo, $G_m(\mathbb{C}^{m+n})$ é identificado com um subconjunto de $L(\mathbb{C}^{m+n}, \mathbb{C}^{m+n}) = \mathbb{C}^{(m+n)^2}$. Ainda, se A é uma matriz geradora de W com colunas ortonormais, então a projeção Π_W é representada pela matriz $[\Pi]_W = A\overline{A}^t$. Observamos que $[\Pi]_W$ é hermitiana e idempotente. A matriz da projeção independe da escolha da matriz geradora. De fato, se A' é outra matriz geradora de $W \in G_m(\mathbb{C}^{m+n})$, então $A' = AV$, com $V \in U(m)$, e segue

$$A'\overline{A'}^t = AV\overline{AV}^t = A(V\overline{V}^t)\overline{A}^t = A\overline{A}^t = [\Pi]_W.$$

Pelo fato de ser hermitiana, a forma geral de uma matriz de projeção $[\Pi]_W$ é

$$\begin{bmatrix} \lambda_1 & a_{11} & ... & a_{1n} \\ \overline{a_{11}} & \lambda_2 & ... & a_{2n} \\ \vdots & \vdots & ... & \vdots \\ \overline{a_{1n}} & \overline{a_{2n}} & ... & \lambda_n \end{bmatrix}, \quad \text{com } \lambda_k \in I\!R \text{ e } a_{ij} \in \mathbb{C}. \tag{4.17}$$

Além disso, usando a matriz geradora na primeira forma de (4.16), temos

$$A\overline{A}^t = \begin{bmatrix} I_m & 0 \\ 0 & 0_n \end{bmatrix},$$

de onde segue $\mathrm{tr}\big([\Pi]_W\big) = m$, para todo $W \in G_m(\mathbb{C}^{m+n})$. Concluímos então que as matrizes de projeção estão num subespaço de $L(\mathbb{C}^{m+n},\mathbb{C}^{m+n})$ de dimensão <u>real</u>

$$d = 2\left(\frac{n^2-n}{2}\right) + n - 1 = n^2 - 1.$$

Considere a *norma de Frobenius* de matrizes em $C^{n\times n}$

$$\|M\|_F := \sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n} |m_{ij}|^2} = \sqrt{\mathrm{tr}\big(M\overline{M}^t\big)}. \tag{4.18}$$

Dados $X, Y \in G_m(\mathbb{C}^{m+n})$ com matrizes geradoras na forma (4.16), temos

$$[\Pi]_X = \begin{bmatrix} I_m & 0 \\ 0 & 0_n \end{bmatrix} \quad \text{e} \quad [\Pi]_Y = \begin{bmatrix} d[\cos^2(\theta_i)]_{m\times m} & d[\cos(\theta_i)\mathrm{sen}(\theta_i)] & 0 \\ d[\cos(\theta_i)\mathrm{sen}(\theta_i)] & d[\mathrm{sen}^2(\theta_i)]_{m\times m} & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

onde $d[\lambda_i]_{p\times p}$ denota a matriz diagonal $p \times p$ com entradas $\lambda_i,\ 1 \le i \le p$. Note que, apesar de representarem projeções em $\mathbb{C}^n$, ambas matrizes possuem entradas reais. Podemos assim calcular diretamente

$$\|[\Pi]_X - [\Pi]_Y\|_F^2 \;=\; \mathrm{tr}\left\{\left([\Pi]_X - [\Pi]_Y\right)\left([\Pi]_X - [\Pi]_Y\right)^t\right\} \;=$$

$$= \;\mathrm{tr}\left([\Pi]_X^2\right) - 2\mathrm{tr}\left([\Pi]_X[\Pi]_Y\right) + \mathrm{tr}\left([\Pi]_Y^2\right) \;=\; p - 2\sum_{i=1}^{m}\cos^2(\theta_i) + \mathrm{tr}\left([\Pi]_Y^2\right).$$

Como

$$[\Pi]_Y^2 = \begin{bmatrix} d[\cos^4(\theta_i) + \cos^2(\theta_i)\text{sen}^2(\theta_i)]_{m\times m} & M & 0 \\ M & d[\text{sen}^4(\theta_i) + \cos^2(\theta_i)\text{sen}^2(\theta_i)]_{m\times m} & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

segue

$$\|[\Pi]_X - [\Pi]_Y\|_F^2 = p - 2\sum_{i=1}^{m}\cos^2(\theta_i) + \sum_{i=1}^{m}\left(\cos^4(\theta_i) + 2\cos^2(\theta_i)\text{sen}^2(\theta_i) + \text{sen}^4(\theta_i)\right) =$$

$$= p - 2\sum_{i=1}^{m}\cos^2(\theta_i) + \sum_{i=1}^{m}\left(\cos^2(\theta_i) + \text{sen}^2(\theta_i)\right)^2 = 2\left(p - \sum_{i=1}^{m}\cos^2(\theta_i)\right).$$

Portanto,

$$\frac{1}{2}\|[\Pi]_X - [\Pi]_Y\|_F^2 = 1 - \cos^2(\theta_1) + ... + 1 - \cos^2(\theta_m) = \sum_{i=1}^{m}\text{sen}^2(\theta_i).$$

Usando a definição (4.14), concluímos que

$$d_c(X,Y) = \frac{1}{\sqrt{2}}\|[\Pi]_X - [\Pi]_Y\|_F. \tag{4.19}$$

Dada a matriz de projeção $[\Pi]_X$, denotamos $[\Pi]'_X = [\Pi]_X - \frac{m}{n}I_n$. Podemos verificar facilmente que $\text{tr}([\Pi]'_X) = 0$ e $\|[\Pi]'_X\|_F^2 = \frac{mn}{n}$, qualquer que seja $X \in G_m(\mathbb{C}^{m+n})$. Feitas estas considerações, temos o seguinte resultado.

Teorema 4.2.1 (Mergulho Esférico [8]) *Considerando a distância cordal d_c em $G_m(\mathbb{C}^{m+n})$, a aplicação*

$$\eta : G_m(\mathbb{C}^{m+n}) \longrightarrow S^{n^2-2}(r) \subset \mathbb{R}^{n^2-1} \tag{4.20}$$

$$X \longmapsto [\Pi]_X - \frac{m}{n}I_n$$

é um mergulho isométrico de $G_m(\mathbb{C}^{m+n})$ na esfera Euclidiana (n^2-2)-dimensional de raio $r = \sqrt{\frac{mn}{2n}}$.

Portanto, a distância cordal entre dois subespaços é igual à $\frac{1}{\sqrt{2}}$ vezes a distância em "linha reta" entre as respectivas matrizes de projeção. Além disso, a medida da

distância entre $X, Y \in G_m(\mathbb{C}^{m+n})$ medida sobre a esfera pode ser calculada usando-se

$$\text{sen}\left(\frac{\theta}{2}\right) = \frac{d_c(X,Y)}{2r} \quad \Rightarrow \quad \theta = 2\text{sen}^{-1}\left(\frac{d_c(X,Y)}{2r}\right) \in [0,\pi],$$

e temos

$$d_s(X,Y) = 2r\text{sen}^{-1}\left(\frac{d_c(X,Y)}{2r}\right).$$

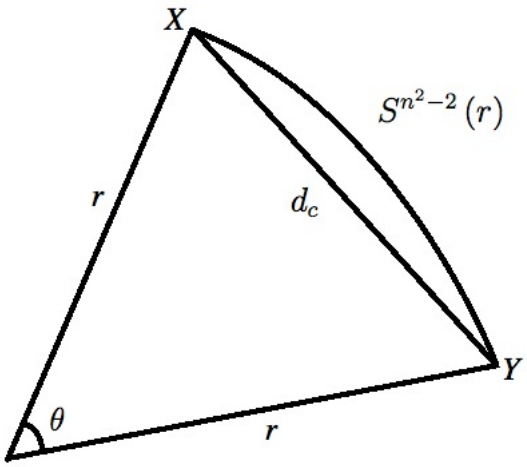

Figura 4.1: Distância cordal na Grassmanniana

De acordo com [18], observamos que não existe um mergulho canônico de uma grassmanniana num espaço $\mathbb{R}^n$, de modo que a distância geodésica d_g seja dada pela restrição da distância euclidiana. Mesmo o *mergulho de Plücker* [3], onde os elementos de $G_m(\mathbb{C}^{m+n})$ são representados por pontos num espaço projetivo de dimensão adequada, não fornece uma maneira de realizar d_g ou d_c por uma distância Euclidiana. A dimensão do mergulho de Plücker é em geral mais alta que a dimensão do mergulho esférico.

Exemplo 4.2.1 (O limitante de Rankin em $G_m(\mathbb{C}^{m+n})$) *Um subconjunto com um número finito $N > 0$ de pontos em $G_m(\mathbb{C}^{m+n})$, de modo que a distância mínima entre quaisquer dois de seus pontos distintos seja $\delta > 0$, será denominado um (N,δ)-código em $G_m(\mathbb{C}^{m+n})$. Vamos considerar a distância cordal (4.14) na variedade de Grassmann. Partindo do mergulho esférico descrito na seção anterior, podemos*

aplicar o limitante de Rankin para códigos esféricos, e assim obter o seguinte resultado para empacotamentos em Grassmannianas.

Para um (N, δ)-código em $G_m(\mathbb{C}^{m+n})$ valem as desigualdades [8]

$$\delta^2 \leq \frac{mn}{m+n}\frac{N}{N-1}, \quad \text{se} \quad N \leq (m+n)^2 \tag{4.21}$$

e

$$\delta^2 \leq \frac{mn}{m+n}, \quad \text{se} \quad (m+n)^2 < N \leq 2((m+n)^2 - 1). \ \square \tag{4.22}$$

Consideremos agora G um grupo de Lie semisimples complexo com álgebra de Lie $\mathfrak{g}$. Escolhendo $\mathfrak{p}$ uma subálgebra parabólica de $\mathfrak{g}$ e denotando por P o subgrupo parabólico definido como o normalizador $N_G(\mathfrak{p})$ de $\mathfrak{p}$ em G, vimos em (3.62) que a variedade flag generalizada é definida pelo quociente

$$\mathcal{F} = \frac{G}{P}.$$

A ação canônica de G em $\mathcal{F}$ é dada por

$$\begin{aligned} G \times \mathcal{F} &\longrightarrow \mathcal{F} \\ (g, hP) &\longmapsto (gh)P \ , \end{aligned}$$

e denotaremos $k = \dim(\mathfrak{p})$.

A ação adjunta de G em $\mathfrak{g}$ induz uma ação de G em $G_k(\mathfrak{g})$ pondo

$$G \times G_k(\mathfrak{g}) \longrightarrow G_k(\mathfrak{g}) \tag{4.23}$$

$$(g, V) \longmapsto \mathrm{Ad}(g)V. \tag{4.24}$$

Como P é o normalizador $N_G(\mathfrak{p})$, fica bem definida a aplicação injetiva

$$i : \mathcal{F} \longrightarrow G_k(\mathfrak{g}) \tag{4.25}$$

$$gP \longmapsto \mathrm{Ad}(g)\mathfrak{p}. \tag{4.26}$$

De fato, para ver que (4.26) está bem definida e é injetiva, observamos que

$$gP = hP \;\Leftrightarrow\; gh^{-1} \in P = N_G(\mathfrak{p}) \;\Leftrightarrow$$
$$\Leftrightarrow\; \mathrm{Ad}(gh^{-1})\mathfrak{p} = \mathfrak{p} \;\Leftrightarrow\; \mathrm{Ad}(g)\mathfrak{p} = \mathrm{Ad}(h)\mathfrak{p}.$$

Com isso podemos considerar a variedade flag $\mathcal{F} = G/P$ como a órbita de $\mathfrak{p}$ em $G_k(\mathfrak{g})$ pela ação adjunta de G.

Fazendo a composição da aplicação i descrita acima com o mergulho esférico η (4.20), obtemos uma nova aplicação

$$j : \mathcal{F} \longrightarrow S^d(r)$$
$$j = \eta \circ i$$

que leva a variedade flag em uma esfera euclidiana de raio e dimensão apropriados.

Portanto, motivados pela definição da distância cordal para grassmannianas, seria natural considerarmos uma nova distância entre pontos $a, b \in \mathcal{F}$ através da distância euclidiana do segmento que une as imagens $j(a)$ e $j(b)$ medida em $\mathbb{R}^{d+1}$. Certamente surgem questões interessantes a serem investigadas, com por exemplo, a relação entre esta nova distância e a distância geodésica em $\mathcal{F}$ proveniente de uma métrica normal. Apesar de serem topologicamente equivalentes, seria possível relacioná-las através uma desigualdade análoga à (4.15) como acontece com δ_g e δ_c em $G_m(\mathbb{C}^n)$? Ainda, o mergulho j permite a aplicação de limitantes já conhecidos para códigos esféricos, como por exemplo o limitante de Rankin, agora para códigos em $\mathcal{F}$ munida desta nova distância. Uma relação quantitativa entre a distância geodésica aqui considerada para flags e esta nova distância de tipo cordal permitiria a investigação de novos limitantes para códigos nestes espaços.

Algumas Perspectivas

- Como destacamos neste trabalho, empacotamentos de esferas nas variedades de Stiefel e Grassmann complexas estão relacionados com sistemas de comunicação *wireless*, mais especificamente, podem ser usados para caracterizar a capacidade de canais MIMO com desvanecimento de Rayleigh em regime de alto SNR, nos casos coerente e não coerente, respectivamente [35]. Desse modo, acreditamos que uma investigação mais detalhada das possíveis aplicações/conexões de códigos em variedades flag com sistemas de comunicação existentes seja uma perspectiva de pesquisa pertinente. Além disso, existe a grande motivação da possibilidade de que, da mesma forma que códigos esféricos possuem um espectro notável de aplicações em diversas áreas, os resultados obtidos possam também ser aplicados em outras áreas do conhecimento.

- No capítulo 3 estudamos distâncias na variedade Grassmann complexa (um caso particular de variedade flag geométrica). Vimos que a distância geodésica δ_g (4.13) e a distância cordal δ_c (4.14), que são de natureza distinta (a saber, a primeira definida de modo intrínseco a partir de uma métrica riemanniana bi-invariante e, a segunda, puramente topológica dada através do mergulho esférico) são relacionadas quantitativamente segundo a Proposição 3.2.1 [33]. Sabendo que a aplicação $i : \mathcal{F} \longrightarrow G_k(\mathfrak{g})$ (4.26) é um mergulho de uma variedade flag numa grassmanniana, podemos considerar uma distância em $\mathcal{F}$ semelhante à cordal, pela composta de i com o mergulho esférico η de $G_k(\mathfrak{g})$. Uma perspectiva natural é a investigação de possíveis relações desta nova distância com a distância geodésica em $\mathcal{F}$.

- Existem trabalhos tais como [28], cujo objetivo é a construção de códigos lineares $\mathcal{C} \subset \mathbb{K}_q^m$ a partir de subconjuntos finitos de uma variedade flag algébrica $\mathcal{F}(\mathbb{K})$. As variedades flag algébricas são definidas de modo análogo às variedades geométricas, apenas trocando-se o corpo $\mathbb{C}$ dos números complexos

por um corpo finito $\mathbb{K}_q$. A construção destes códigos é feita usando-se um mergulho de $\mathcal{F}(\mathbb{K})$ num espaço projetivo de dimensão grande, obtendo-se assim um *sistema projetivo* [15]. Acreditamos que é possível melhorar a construção apresentada em [28] usando uma adaptação do mergulho $i : \mathcal{F} \longrightarrow G_k(\mathfrak{g})$ (4.26) para o caso algébrico, juntamente com o *mergulho de Plücker* [18]. A perspectiva é a obtenção de códigos com boas propriedades e melhores taxas devido à menor dimensão do espaço projetivo de chegada.

- Pesquisar o problema do raio de cobertura, que é dual ao problema do empacotamento considerado aqui. Ou seja, dado $\rho > 0$, minimizar o número de pontos $|\mathcal{C}|$ de códigos $\mathcal{C} \subset \mathcal{M}$ tais que

$$\bigcup_{c_i \in \mathcal{C}} B_\rho(c_i) = \mathcal{M}, \tag{4.27}$$

  onde $\mathcal{M}$ é uma variedade flag.

- Dada uma variedade flag $\mathcal{F}$, ou até mesmo um espaço homogêneo qualquer $\mathcal{M} = \frac{G}{H}$, estudar propriedades de códigos em $\mathcal{M}$ que são órbitas de subgrupos discretos do grupo de Lie G.

Apêndice A

Grupos e Álgebras de Lie

A.1 Grupos de Lie

Definição A.1.1 *Um* **grupo de Lie** G *é um grupo munido de uma estrutura de variedade diferenciável, de modo que o produto*

$$\begin{aligned} p : G \times G &\longrightarrow G \\ (g, h) &\longmapsto gh \end{aligned}$$

e a inversão

$$\begin{aligned} i : G &\longrightarrow G \\ g &\longmapsto g^{-1} \end{aligned}$$

são aplicações diferenciáveis.

Exemplo A.1.1 (O Grupo Linear) *Seja $GL(n, \mathbb{R})$ o grupo das transformações lineares inversíveis do $\mathbb{R}^n$, com a operação de composição. Fixada uma base do $\mathbb{R}^n$, $GL(n, \mathbb{R})$ torna-se o grupo das matrizes reais inversíveis de tamanho $n \times n$, com a operação de produto. Trata-se de um subgrupo de $\mathbb{R}^{n \times n}$. Além disso,*

$$GL(n, \mathbb{R}) = \{A \in \mathbb{R}^{n \times n} : \det(A) \neq 0\}$$

é um subconjunto aberto de $\mathbb{R}^{n \times n}$, pois a função determinante é contínua. Como $\mathbb{R}^{n \times n} \approx \mathbb{R}^{n^2}$ é variedade diferenciável, segue que $GL(n, \mathbb{R})$ é uma subvariedade aberta. Finalmente, o produto de matrizes $(A, B) \longmapsto AB$ é diferenciável, pois é dado em coordenadas através de funções polinomiais, e a diferenciabilidade da inversão

$A \longmapsto A^{-1}$ segue da regra de Cramer. Concluímos assim que $GL(n, \mathbb{R})$ é um grupo de Lie. $\square$

Se G é um grupo de Lie, a *translação à esquerda* associada ao elemento $g \in G$ é a aplicação $L_g : G \longrightarrow G$ dada por $L_g(h) = gh$, para qualquer $h \in G$. Analogamente, podemos definir as *translações à direita* em G. Em ambos os casos, a definição de grupo de Lie implica que as translações são difeomorfismos de G.

Definição A.1.2 *Um subgrupo H é um* **subgrupo de Lie** *de um grupo de Lie G se H é uma subvariedade (não necessariamente mergulhada) de G, e o produto e a inversão de H são diferenciáveis em relação à estrutura intrínseca de H.*

O seguinte teorema, devido a E. Cartan, fornece uma caracterização muito importante e útil para determinarmos os subgrupos de Lie de um grupo de Lie G.

Teorema A.1.1 (Cartan) *Se H é um subgrupo fechado de um grupo de Lie G, então H é um subgrupo de Lie.*

Na verdade, o resultado mais geral dá uma caracterização para os subgrupos mergulhados de G: um subgrupo H é uma subvariedade mergulhada de G se, e somente se, H é fechado.

Exemplo A.1.2 *O grupo*

$$SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : \det(A) = 1\}$$

é um subgrupo de Lie de $GL(n, \mathbb{R})$, pois trata-se de um subconjunto fechado. De fato, $SL(n, \mathbb{R}) = \det^{-1}(\{1\})$, e o conjunto discreto $\{1\} \subset \mathbb{R}$ é fechado. Outros exemplos importantes de subgrupos de Lie de $GL(n, \mathbb{R})$ são

- $O(n) = \{A \in GL(n, \mathbb{R}) : A^t = A^{-1}\}$;
- $SO(n) = \{A \in GL(n, \mathbb{R}) : \det(A) = 1\}$;
- $SP(n, \mathbb{R}) = \{A \in GL(2n, \mathbb{R}) : AJA^t = J\}$, *onde* $J = \begin{bmatrix} 0 & 1_n \\ 1_n & 0 \end{bmatrix}$.

Definição A.1.3 *Seja H um subconjunto de um grupo de Lie G. O* **centralizador** *e o* **normalizador** *de H em G são definidos respectivamente por*

$$Z_G(H) := \{g \in G : gh = hg, \ \forall h \in H\} \tag{A.1}$$

e

$$N_G(H) := \{g \in G : gHg^{-1} = H\}. \tag{A.2}$$

Se H é um subgrupo de G, então seu normalizador e seu centralizador também são subgrupos. O centralizador $Z_G(H)$ é um subgrupo fechado, e assim, um subgrupo de Lie de G. Ainda, se H é fechado pode-se mostrar que $N_G(H)$ também é, sendo assim um subgrupo de Lie.

Definição A.1.4 *Dados G e H grupos de Lie, uma aplicação $\phi : G \longrightarrow H$ é chamada de* **homorfismo de grupos de Lie** *se é um homomorfismo (no sentido usual) e também é contínua. Se ϕ admite uma inversa contínua, dizemos que ϕ é um* **isomorfismo de grupos de Lie**.

Nesse ponto é importante observarmos que a continuidade do homomorfismo ϕ garante que ele também é C^∞ [29]. Se $G = H$ na definição acima, então chamamos um isomorfismo de grupos de Lie de *automorfismo* de G.

A.2 Álgebras de Lie

Definição A.2.1 *Uma* **álgebra de Lie** $\mathfrak{g} = (V, [\ ,\ ])$ *é um par formado por um espaço vetorial V de dimensão finita sobre um corpo $\mathbb{K}$, e um produto (denominado* **colchete de Lie***)*

$$(X, Y) \longmapsto [X, Y] \in V \tag{A.3}$$

bilinear, anti-simétrico e satisfazendo a identidade de Jacobi

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0. \tag{A.4}$$

Neste trabalho, o corpo $\mathbb{K}$ da definição acima sempre será o conjunto dos números reais $\mathbb{R}$ ou o conjunto dos números complexos $\mathbb{C}$.

Exemplo A.2.1 *Vamos agora apresentar alguns exemplos importantes de álgebras de Lie.*

1. *Qualquer espaço vetorial V com o colchete trivial $[X, Y] = 0$, é uma álgebra de Lie. Estas são chamadas* **álgebras abelianas**. *De fato, se o colchete for comutativo, então a anti-simetria implicará $[X, Y] = 0,\ \forall X, Y \in V$.*

2. *Seja $\mathfrak{A}$ uma álgebra sobre $\mathbb{R}$ ou $\mathbb{C}$ (isto é, um espaço vetorial real ou complexo, com uma multiplicação associativa XY). Então podemos tornar $\mathfrak{A}$ uma álgebra de Lie definindo o colchete*

$$[X, Y] = XY - YX, \tag{A.5}$$

chamado **produto comutador**. *Quando $\mathfrak{A}$ é a álgebra dos operadores do espaço vetorial V, com o produto dado pela composição, a álgebra de Lie correspondente é chamada* **álgebra linear geral** *de V, e notada $\mathfrak{gl}(V)$. Se $V = \mathbb{R}^n$ então $\mathfrak{A} = \mathbb{R}^{n\times n}$, e a álgebra de Lie neste caso é denotada $\mathfrak{gl}(n, \mathbb{R})$. De modo análogo, podemos definir $\mathfrak{gl}(n,\mathbb{C})$.*

3. *A* **álgebra especial linear** *$\mathfrak{sl}(n, \mathbb{R})$, consiste de todas as matrizes reais com traço nulo*

$$\mathfrak{sl}(n, \mathbb{R}) = \{A \in \mathfrak{gl}(n.\mathbb{R}) : \mathrm{tr}(A) = 0\}, \tag{A.6}$$

com o colchete herdado de $\mathfrak{gl}(n, \mathbb{R})$. Neste caso, diremos que $\mathfrak{sl}(n, \mathbb{R})$ é uma subálgebra de Lie de $\mathfrak{gl}(n, \mathbb{R})$.

4. *Tome V um espaço vetorial, e seja β uma forma bilinear não degenerada em V. A* **álgebra de Lie ortogonal** *$\mathfrak{o}(V, \beta)$ é dada pelos operadores T em V que satisfazem*

$$\beta(TX, Y) + \beta(X, TY) = 0, \tag{A.7}$$

(ou equivalentemente $\beta(TX, X) = 0$) para quaisquer $X, Y \in V$, com o colchete herdado de $\mathfrak{gl}(V)$. Se $V = \mathbb{K}^n$, adotamos $\beta(X, Y) = X^tY = \sum_{i=1}^n x_iy_i$, e a álgebra de Lie correspondente é denotada $\mathfrak{o}(n, \mathbb{K})$. Se $T \in \mathfrak{o}(n, \mathbb{K})$, então pode-se mostrar que $X^t(T^t + T)Y = 0,\ \forall X, Y \in \mathbb{K}^n$, e concluímos que $\mathfrak{o}(n, \mathbb{K})$ é o conjunto formado pelas matrizes anti-simétricas, isto é, satisfazendo $T^t+T = 0$. Quando $\mathbb{K} = \mathbb{R}$ temos o caso clássico, denotado simplesmente por $\mathfrak{o}(n)$.

5. *Seja V um espaço vetorial complexo, e tome λ um produto interno hermitiano em V. A* **álgebra de Lie unitária** *$\mathfrak{u}(V, \lambda)$ consite de todos os operadores T em V tais que*

$$\lambda(TX, Y) + \lambda(X, TY) = 0, \tag{A.8}$$

para quaisquer $X, Y \in V$. É muito importante observar que, apesar de ser definida por um espaço vetorial complexo, esta é uma álgebra de Lie real. De fato, se T é invariante então αT também é, para todo $\alpha \in \mathbb{R}$; contudo $\sqrt{-1}T$

não é. Se $V = \mathbb{C}^n$ *e* $\lambda(X,Y) := \langle X,Y\rangle = \sum_{i=1}^n x_i y_i$*, obtemos a álgebra de Lie* $\mathfrak{u}(n)$*, formada por todas as matrizes anti-hermitianas. Isto é, matrizes* $M \in \mathbb{C}^{n\times n}$ *satisfazendo* $\overline{M}^t + M = 0$*. Finalmente, existe também a* **álgebra de Lie especial unitária** $\mathfrak{su}(n)$*, formada por todos os elementos de* $\mathfrak{u}(n)$ *que tem traço nulo.*

6. *Sejam* V *um espaço vetorial sobre* $\mathbb{K}$ *e* Ω *uma forma bilinear, anti-simétrica e não degenerada em* V*. A* **álgebra de Lie simplética** $\mathfrak{sp}(V,\Omega)$ *é formada pelos operadores* T *em* V *que satisfazem*

$$\Omega(TX,Y) + \Omega(X,TY) = 0, \tag{A.9}$$

para quaisuquer $X, Y \in V$*. Escrevemos* $\mathfrak{sp}(n,\mathbb{R})$ *ou* $\mathfrak{sp}(n,\mathbb{C})$ *para as álgebras de Lie simpléticas de* $\mathbb{R}^{2n}$ *ou* $\mathbb{C}^{2n}$*, dadas pela forma bilinear*

$$\Omega(X,Y) = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 + ... + x_{2n-1}y_{2n} - x_{2n}y_{2n-1}.$$

Sabe-se que a forma bilinear acima é não degenerada desde que a dimensão de V *seja par, e também que toda forma bilinear anti-simétrica definida em* $\mathbb{R}^{2n}$ *ou* $\mathbb{C}^{2n}$ *pode ser escrita como a expressão acima, a menos de uma mudança de base. Se*

$$J_1 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad \text{e} \qquad J = \text{diag}(J_1, ..., J_1)$$

então esta álgebra pode ser descrita como o conjunto das matrizes $M \in \mathbb{K}^{2n\times 2n}$ *que satisfazem* $M^tJ = -JM$*. Finalmente, as matrizes que estão simultâneamente em* $\mathfrak{sp}(n,\mathbb{C})$ *e* $\mathfrak{u}(2n)$ *formam uma álgebra de Lie real, denotada simplesmente* $\mathfrak{sp}(n)$*.*

Vamos introduzir a simbologia padrão para algumas destas álgebras:

- $\mathfrak{a}_n = \mathfrak{sl}(n+1,\mathbb{C})$, para $n = 1, 2, 3, ...$
- $\mathfrak{b}_n = \mathfrak{o}(2n+1,\mathbb{C})$, para $n = 2, 3, 4, ...$
- $\mathfrak{c}_n = \mathfrak{sp}(n,\mathbb{C})$, para $n = 3, 4, 5, ...$
- $\mathfrak{d}_n = \mathfrak{o}(2n,\mathbb{C})$, para $n = 4, 5, 6, ...$

As álgebras $\mathfrak{a}_n$, $\mathfrak{b}_n$, $\mathfrak{c}_n$ e $\mathfrak{d}_n$ são as quatro famílias de álgebras de Lie *semi-simples complexas*, e serão discutidas mais detalhadamente na subseção A.2.4. Tais álgebras

são importantes em nosso estudo, pois as variedades flag são definidas a partir delas.

Considere $\mathcal{X}^1(\mathcal{M})$ o conjunto dos campos de vetores diferenciáveis numa variedade $\mathcal{M}^n$. Assim $X \in \mathcal{X}^1(\mathcal{M})$ é uma aplicação diferenciável de $\mathcal{M}$ no fibrado $T\mathcal{M}$, tal que $\pi \circ X = I_{\mathcal{M}}$. Fixada uma parametrização $x = (x_1, ..., x_n)$ de $\mathcal{M}$ em $p \in \mathcal{M}$, podemos escrever

$$X(p) = \sum_{i=1}^{n} a_i(p) \frac{\partial}{\partial x_i},$$

onde cada a_i é uma função real diferenciável e $\left\{\frac{\partial}{\partial x_i}\right\}$ é a base do espaço tangente associada à parametrização x. Podemos pensar em um campo $X \in \mathcal{X}^1(\mathcal{M})$ como uma aplicação do conjunto das funções diferenciáveis em $\mathcal{M}$, definida do seguinte modo

$$(Xf)(p) = \sum_{i=1}^{n} a_i(p) \frac{\partial f}{\partial x_i}(p),$$

onde f indica, a expressão de f na parametrização x. Ou seja, cada campo de vetores é interpretado como uma derivada direcional. Vale que, dados dois campos X e Y em $\mathcal{X}^1(\mathcal{M})$, existe um único campo $Z \in \mathcal{X}^1(\mathcal{M})$ tal que, para toda função diferenciável f de $\mathcal{M}$, tem-se

$$Zf = (XY - YX)f.$$

Denotamos $Z = [X, Y]$, e de fato vale a anti-comutatividade, a bilinearidade e a identidade de Jacobi (A.4). Portanto, $\mathcal{X}^1(\mathcal{M})$ munido do colchete $[X, Y] = XY - YX$ é uma álgebra de Lie, denominada *álgebra dos campos vetoriais* da variedade $\mathcal{M}$.

Definição A.2.2 *Um subespaço vetorial $\mathfrak{h}$ de uma álgebra de Lie $\mathfrak{g}$ é chamado de* **subálgebra de Lie**, *se é fechado pelo colchete. Ou seja, $X, Y \in \mathfrak{h}$ implica que $[X, Y] \in \mathfrak{h}$.*

Definição A.2.3 *Uma transformação linear entre álgebras de Lie $\psi : \mathfrak{g} \longrightarrow \mathfrak{h}$ é chamada de* **homomorfismo de álgebras de Lie** *se $\psi[X, Y] = [\psi X, \psi Y]$, para quaisquer $X, Y \in \mathfrak{g}$. Se ela também for inversível, então dizemos que ψ é um* **isomorfismo de álgebras de Lie**.

Conforme definimos anteriormente para grupos, se $\mathfrak{g} = \mathfrak{h}$, dizemos que ψ é um *automorfismo* de $\mathfrak{g}$. Como veremos mais adiante, cada homomorfismo de grupos de Lie induz um homomorfismo de álgebras de Lie.

Definição A.2.4 *Um subespaço $\mathfrak{h}$ de uma álgebra de Lie $\mathfrak{g}$ é um* **ideal** *se para quaisquer $Y \in \mathfrak{h}$, $X \in \mathfrak{g}$ vale $[X, Y] \in \mathfrak{h}$. Ou seja,*

$$[\mathfrak{g}, \mathfrak{h}] = \{[X, Y] : X \in \mathfrak{g}, Y \in \mathfrak{h}\} \subseteq \mathfrak{h}.$$

Segue imediatamente que se $\psi : \mathfrak{g} \longrightarrow \mathfrak{h}$ é um homomorfismo de álgebras de Lie, então seu núcleo $\mathfrak{Ker}(\psi)$ é um ideal de $\mathfrak{g}$, e sua imagem $\mathfrak{Im}(\psi)$ uma subálgebra de $\mathfrak{h}$. Se $\mathfrak{h} \subseteq \mathfrak{g}$ é um ideal, munimos o espaço vetorial quociente $\mathfrak{g}/\mathfrak{h}$ com uma estrutura de álgebra de Lie definindo o colchete $[\overline{X}, \overline{Y}] = \overline{[X, Y]}$. De fato, esta definição não depende dos representantes escolhidos e a projeção canônica

$$\begin{aligned} \pi : \mathfrak{g} &\longrightarrow \mathfrak{g}/\mathfrak{h} \\ X &\longmapsto \overline{X} \end{aligned}$$

é um homomorfismo sobrejetor. Também vale o *Teorema de Isomorfismo*, que afirma que $\mathfrak{g}/\mathfrak{Ker}(\psi) \approx \mathfrak{Im}(\psi)$, se $\psi : \mathfrak{g} \longrightarrow \mathfrak{h}$ é um homomorfismo.

Definição A.2.5 *Seja V um espaço vetorial e denote por $\mathfrak{gl}(V)$ a álgebra de Lie das transformações lineares de V. Se $\mathfrak{g}$ é uma álgebra de Lie sobre o mesmo corpo de escalares, um homomorfismo $\rho : \mathfrak{g} \longrightarrow \mathfrak{gl}(V)$ é chamado de* **representação** *de $\mathfrak{g}$ em V. Uma representação ρ é dita* **fiel** *se $\mathfrak{Ker}(\rho) = \{0\}$.*

Analogamente, definimos uma **representação** do grupo de Lie G em V como um homomorfismo entre grupos de Lie de G em $GL(V)$.

Uma representação notável de grupos de Lie é a chamada *representação adjunta*. Trata-se de uma representação do grupo G em sua álgebra de Lie $\mathfrak{g}$, definida do seguinte modo. Para $g \in G$, considere a aplicação $C_g : G \longrightarrow G$ (denominada *conjugação*) dada por

$$G_g(h) := ghg^{-1}, \ \forall h \in G.$$

Sua diferencial no elemento neutro de G é uma transformação linear $d(C_g)_1 : \mathfrak{g} \longrightarrow \mathfrak{g}$, e será denotada $\mathrm{Ad}(g)$. Fazendo isso para cada elemento de G, obtemos a representação

$$\begin{aligned} \mathrm{Ad} : G &\longrightarrow GL(\mathfrak{g}) \\ g &\longmapsto \mathrm{Ad}(g). \end{aligned} \tag{A.10}$$

Por outro lado, a *representação adjunta* de uma álgebra de Lie $\mathfrak{g}$

$$\mathrm{ad} : \mathfrak{g} \longrightarrow \mathfrak{gl}(\mathfrak{g})$$

é a aplicação que associa a cada $X \in \mathfrak{g}$ a transformação linear $\mathrm{ad}(X) : \mathfrak{g} \longrightarrow \mathfrak{g}$ dada por

$$\mathrm{ad}(X)(Y) = [X, Y], \ \forall Y \in \mathfrak{g}. \tag{A.11}$$

Segue imediatamente da bilinearidade do colchete que $\mathrm{ad}(X)$ é linear. Ainda

$$\begin{gathered}
\mathrm{ad}([X,Y]) = \mathrm{ad}(X)\mathrm{ad}(Y) - \mathrm{ad}(Y)\mathrm{ad}(X), \forall X, Y \in \mathfrak{g} \Leftrightarrow \\
\Leftrightarrow \mathrm{ad}([X,Y])(Z) = (\mathrm{ad}(X) \circ \mathrm{ad}(Y))(Z) - (\mathrm{ad}(Y) \circ \mathrm{ad}(X))(Z), \forall X, Y, Z \in \mathfrak{g} \Leftrightarrow \\
\Leftrightarrow [[X,Y],Z] = [X,[Y,Z]] - [Y,[X,Z]], \forall X, Y, Z \in \mathfrak{g} \Leftrightarrow \\
\Leftrightarrow [X,[Y,Z]] = [[X,Y],Z] + [Y,[X,Z]], \ \forall X, Y, Z \in \mathfrak{g}
\end{gathered}$$

que é justamente a identidade de Jacobi, donde concluímos que ad é um homomorfismo de álgebras de Lie.

Proposição A.2.1 *A representação* $\mathrm{Ad} : G \longrightarrow GL(\mathfrak{g})$ *é diferenciável, e sua diferencial no elemento neutro de* G *é* $\mathrm{ad} : \mathfrak{g} \longrightarrow \mathfrak{gl}(\mathfrak{g})$. *Ou seja,*

$$\mathrm{ad}(X) = d(\mathrm{Ad})_1(X), \ \forall x \in \mathfrak{g}.$$

Definição A.2.6 *Dado um subconjunto* $\mathfrak{h}$ *de uma álgebra de Lie* $\mathfrak{g}$*, definimos seu* **centralizador** *e seu* **normalizador** *respectivamente por*

$$\mathfrak{z}(\mathfrak{h}) := \{X \in \mathfrak{g} : [X, Y] = 0, \ \forall Y \in \mathfrak{h}\} \tag{A.12}$$

e

$$\mathfrak{n}(\mathfrak{h}) := \{X \in \mathfrak{g} : [X, \mathfrak{h}] \subseteq \mathfrak{h}\}. \tag{A.13}$$

Se $\mathfrak{h}$ for uma subálgebra de Lie de $\mathfrak{g}$ então seu centralizador e seu normalizador também são subálgebras. Ainda, o núcleo da representação adjunta é $\mathfrak{z}(\mathfrak{g})$, chamado de *centro* de $\mathfrak{g}$.

A.3 Relação entre Grupos e Álgebras de Lie

Suponha que $\mathcal{M}$ e $\mathcal{N}$ são variedades diferenciáveis e que X é um campo de vetores em $\mathcal{M}$. Se $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ é um difeomorfismo, podemos transladar X a um campo $\phi_* X$ em $\mathcal{N}$ definido por

$$(\phi_* X)(y) = d\phi_{\phi^{-1}(y)}(X(\phi^{-1}(y))),$$

para todo $y \in \mathcal{N}$. Vale que $\phi_*[X, Y] = [\phi_* X, \phi_* Y]$ para quaisquer campos X, Y de $\mathcal{M}$, onde $[\ ,\ ]$ denota o colchete de Lie de campos de vetores.

Um campo de vetores X em um grupo de Lie G é dito *invariante à esquerda* se para todo $g \in G$ vale $(L_g)_* X = X$, ou seja, $d(L_g)_h(X(h)) = X(gh)$ para todos $g, h \in G$. Analogamente, poderíamos definir campos invariantes à direita. Contudo só trataremos aqui de campos invariantes à esquerda, e neste caso, diremos apenas *campo invariante*.

Os campos invariantes são completamente determinados por seu valor no elemento identidade $1 \in G$, pois para todo $g \in G$, temos $X(g) = d(L_g)_1(X(1))$. Desse modo, todo elemento do espaço tangente $T_1 G$ determina um campo de vetores invariante em G. Mais ainda, existe um isomorfismo entre $T_1 G$ e o conjunto dos campos de vetores invariantes (à direita ou à esquerda) do grupo de Lie G. Com estas considerações, estamos prontos para nossa próxima definição.

Definição A.3.1 *Dado um grupo de Lie G, a* **álgebra de Lie associada** $\mathfrak{g} = \mathfrak{Lie}(G)$ *é definida como o espaço tangente de G no elemento neutro, munido do colchete de campos de vetores. Isto é,*

$$\mathfrak{Lie}(G) := T_1 G. \tag{A.14}$$

Um comentário pertinente à definição acima é que, dados dois elementos $X, Y \in T_1 G$, o colchete $[X, Y]$ é por definição $[\tilde{X}, \tilde{Y}](1)$, onde $\tilde{X}$ e $\tilde{Y}$ são os campos invariantes em G obtidos de X e Y, respectivamente.

Para as álgebras de Lie apresentadas na subseção anterior, temos os respectivos grupos:

1. O **grupo linear geral** $GL(n, \mathbb{K})$, formado por todas as matrizes inversíveis com entradas em $\mathbb{K}$.

2. O **grupo linear especial** $SL(n, \mathbb{K})$, formado por todas as matrizes em $GL(n, \mathbb{K})$ com determinante igual a 1.

3. O **grupo ortogonal** $O(n, \mathbb{K})$, formado pelas matrizes em $M \in GL(n, \mathbb{K})$ tais que $M^t M = 1$. Temos ainda o **grupo especial ortogonal**

$$SO(n, \mathbb{K}) = O(n, \mathbb{K}) \cap SL(n, \mathbb{K}).$$

4. O **grupo unitário** $U(n)$ consiste de todas as matrizes $M \in \mathbb{C}^{n\times n}$ tais que $\overline{M}^t M = 1$, e o **grupo especial unitário** é definido por

$$SU(n) = U(n) \cap SL(n,\mathbb{C}).$$

5. O **grupo simplético** $SP(n, \mathbb{K})$ é formado por todas as matrizes $M \in \mathbb{K}^{2n\times 2n}$ tais que $M^t J M = J$. Estas matrizes necessariamente tem determinante igual a 1. Finalmente, $SP(n) = SP(n,\mathbb{C}) \cap U(2n)$ é o grupo simplético clássico.

Todos os conjuntos acima são subvariedades do espaço vetorial $\mathbb{K}^{n^2} = M_{n\times n}(\mathbb{K})$, definidos por um número finito de equações. Além disso, $O(n)$, $SO(n)$, $U(n)$, $SU(n)$ e $SP(n)$ são compactas, isto é, fechadas e limitadas dentro de seus respectivos espaços $\mathbb{R}^{n^2}$ ou $\mathbb{C}^{n^2}$.

A função exponencial real usual e^t é um homomorfismo diferenciável de $\mathbb{R} = \mathfrak{gl}(1, \mathbb{R})$ em $GL^+(1, \mathbb{R})$, o grupo multiplicativo dos números reais positivos. Mais geralmente, se X é qualquer matriz em $\mathfrak{gl}(n, \mathbb{R})$, sabe-se então que a série

$$\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!} \tag{A.15}$$

converge em $GL(n, \mathbb{R})$. Valem as propriedades

- $\det(\exp(X)) = e^{\mathrm{tr}(X)} > 0$,
- $\exp(X + Y) = \exp(X)\exp(Y)$,

para quaisquer $X, Y \in \mathfrak{gl}(n, \mathbb{R})$. Estes exemplos são casos particulares da aplicação exponencial entre álgebras e grupos de Lie, cuja definição geral é dada como se segue.

O próximo exemplo exibe mais detalhadamente como se estabelece esta relação.

Exemplo A.3.1 (O Grupo Especial Unitário) *Considere o grupo de Lie*

$$SU(n) = \{A \in GL(n,\mathbb{C}) : A\overline{A}^t = \overline{A}^t A = 1_n \text{ e } \det(\mathrm{A}) = 1\}.$$

Ele é um subgrupo de Lie de $U(n)$, o grupo das matrizes unitárias. Considere $\alpha : \mathbb{R} \longrightarrow SU(n)$ uma curva diferenciável tal que $\alpha(0) = 1_n$. Desse modo temos $\det(\alpha(t)) = 1,\ \forall t \in \mathbb{R}$; e derivando no instante $t = 0$ resulta

$$\det{}'(\alpha(t)).\alpha'(t)\Big|_{t=0} = 0 \quad \Rightarrow \quad \det{}'(1_n).\alpha'(0) = 0.$$

Lembrando que

$$\det : \mathfrak{gl}(n,\mathbb{C}) \simeq \mathbb{C}^n \times ... \times \mathbb{C}^n \longrightarrow \mathbb{C}$$

é uma aplicação n-linear, temos $\det{}'(1_n)(X) = \det{}'(e_1, ..., e_n)(X_1, ..., X_n)$ onde $e_i = (0, ..., 0, 1, 0, ..., 0)$ são os vetores da base canônica de $\mathbb{C}^n$ e X_i os vetores coluna da matriz X. Então

$$\det{}'(1_n)(X) = \sum_{i=1}^{n} \det(B_i),$$

onde B_i é a matriz obtida substituindo a i-ésima coluna da matriz identidade pela i-ésima coluna de X. Segue, por uma mudança de linhas e colunas, que $\det{}'(1_n).\alpha'(0) = \mathrm{tr}(\alpha'(0)) = 0$. Portanto

$$T_{1_n}[SU(n)] \subseteq \{A \in \mathfrak{gl}(n,\mathbb{C}) : \mathrm{tr}(A) = 0\}.$$

Por outro lado, se $\mathrm{tr}(A) = 0$ definimos a curva $\alpha(t) = \exp(tA)$, para $t \in \mathbb{R}$. Então α é diferenciável, e é imediato verificar que $\alpha(t) \in SU(n)$, para todo $t \in \mathbb{R}$. Ainda, derivando no instante $t = 0$, obtemos

$$\alpha'(t)\Big|_{t=0} = \exp(0).A = A.$$

Logo $T_{1_n}[SU(n)] = \{A \in \mathfrak{gl}(n,\mathbb{C}) : \mathrm{tr}(A) = 0\}$, e esta álgebra de Lie será denotada $\mathfrak{su}(n)$. Trata-se de uma subálgebra de $\mathfrak{gl}(n,\mathbb{C})$, com o colchete dado pelo comutador

$[X, Y] = XY - YX$. $\square$

Um *subgrupo a um parâmetro* de um grupo de Lie G é um homomorfismo diferenciável $u : I\!R \longrightarrow G$. Sua diferencial $d_0(u)$ é uma aplicação linear de $I\!R$ num subespaço da álgebra de Lie $T_1(G) = \mathfrak{g}$. Decorre do teorema de existência e unicidade de soluções de EDO's que a aplicação $u \longmapsto d_0(u)(1)$ é uma bijeção entre o conjunto dos subgrupos a um parâmetro de G e sua álgebra de Lie $\mathfrak{g}$. De fato, para cada $X \in T_1\mathrm{G}$ existe um único subgrupo a um parâmetro u_X de G tal que $d_0(u_X)(1) = X$.

Definição A.3.2 *Dado um grupo de Lie G com álgebra associada $\mathfrak{g}$, definimos sua* **aplicação exponencial** $\exp_G : \mathfrak{g} \longrightarrow G$ *por*

$$\exp_G(X) = u_X(1). \tag{A.16}$$

Ou seja, $\exp_G(X)$ é o valor em $1 \in G$ da solução da EDO gerada por X que passa pelo elemento neutro no instante $t = 0$.

Proposição A.3.1 *[29] Se $\phi : G \longrightarrow H$ é um homomorfismo de grupos de Lie, então sua diferencial no elemento neutro $d\phi_1 : \mathfrak{g} \longrightarrow \mathfrak{h}$ é um homomorfismo entre as álgebras de Lie de G e H. Além disso*

$$\phi(\exp_G(X)) = \exp_{\mathrm{H}}(d\phi_1(X)).$$

Ou seja, o seguinte diagrama é comutativo.

$$\begin{array}{ccc} \mathfrak{g} & \xrightarrow{d\phi_1} & \mathfrak{h} \\ {\scriptstyle \exp_G}\downarrow & & \downarrow{\scriptstyle \exp_H} \\ G & \xrightarrow[\phi]{} & H \end{array}$$

Desta proposição, obtemos as importantes fórmulas

$$g\exp_G(X)g^{-1} = \mathrm{Ad}(g)(X) \tag{A.17}$$

e

$$\mathrm{Ad}(\exp_G(X)) = \exp_G(\mathrm{ad}(X)) \tag{A.18}$$

para todo $X \in \mathfrak{g}$.

Proposição A.3.2 *[29] Valem as seguintes afirmações:*

1. *Se X é um campo de vetores invariante à esquerda, então seu fluxo é $X_t = D_{\exp_G(tX)}$. Isto é,*
$$X_t(g) = g\exp_G(tX);$$
2. $\exp_G(0) = 1$;
3. *Para quaisquer $X \in \mathfrak{g}$ e $t, s \in \mathbb{R}$ vale*
$$\exp_G(t+s)X = \exp_G(tX)\exp_G(sX) = \exp_G(sX)\exp_G(tX).$$
Isto é, os elementos do subgrupo $\{\exp_G(tX) : t \in \mathbb{R}\}$ comutam entre si;
4. *Para $X, Y \in \mathfrak{g}$, vale*
$$[X,Y] = 0 \quad \Leftrightarrow \quad \exp_G(tX)\exp_G(sY) = \exp_G(sY)\exp_G(tX).$$

Proposição A.3.3 *Seja G um grupo de Lie, com álgebra de Lie $\mathfrak{g}$. Então temos*

$$d(\exp_G)_0 = I_{\mathfrak{g}}. \tag{A.19}$$

Segue pelo teorema da função inversa que a aplicação exponencial $\exp_G$ é um difeomorfismo entre uma vizinhança de $0 \in \mathfrak{g}$ e uma vizinhança de $1 \in G$. Se G é um grupo conexo, então para qualquer vizinhança V do elemento neutro, temos que $G = \cup_{n\geq 1} V^n$. Sendo $\exp_G$ um difeomorfismo numa vizinhança de 0, todo elemento $g \in G$ pode ser escrito como um produto de exponenciais. Isto é

$$g = \exp_G(X_1)\exp_G(X_2)...\exp_G(X_n), \text{ com } X_1, X_2, ..., X_n \in \mathfrak{g}.$$

Definição A.3.3 *Seja G um grupo de Lie com álgebra de Lie $\mathfrak{g}$, e considere $\mathfrak{h} \subset \mathfrak{g}$ uma subálgebra. O* **normalizador** *e o* **centralizador** *de $\mathfrak{h}$ em G são definidos, respectivamente, como os subgrupos*

$$N_G(\mathfrak{h}) := \{g \in G : \mathrm{Ad}(g)\mathfrak{h} = \mathfrak{h}\}$$

e

$$Z_G(\mathfrak{h}) := \{g \in G : \mathrm{Ad}(g)H = H, \ \forall H \in \mathfrak{h}\}.$$

Proposição A.3.4 *Vale que* $\mathfrak{Lie}\,[N_G(\mathfrak{h})] = \mathfrak{n}(\mathfrak{h})$ *e* $\mathfrak{Lie}\,[Z_G(\mathfrak{h})] = \mathfrak{z}(\mathfrak{h})$. *Além disso, se* H *é um grupo de Lie conexo com álgebra* $\mathfrak{h}$ *então valem as igualdades*

$$Z_G(\mathfrak{h}) = Z_G(H) \quad \text{e} \quad N_G(\mathfrak{h}) = N_G(H).$$

A.4 Subálgebras de Cartan, Raízes

Definição A.4.1 *A* **forma de Cartan-Killing** *de uma álgebra de Lie* $\mathfrak{g}$ *(de dimensão finita) é a forma bilinear simétrica* $\langle\ ,\ \rangle_{CK} : \mathfrak{g} \times \mathfrak{g} \longrightarrow I\!K$ *dada por*

$$\langle X, Y\rangle_{CK} = \operatorname{tr}\left(\operatorname{ad}(X)\operatorname{ad}(Y)\right). \tag{A.20}$$

Sabemos que toda álgebra de Lie $\mathfrak{g}$ possui um único ideal maximal solúvel, chamado *radical* de $\mathfrak{g}$, que será denotado $\mathfrak{r}$.

Definição A.4.2 *Uma álgebra de Lie* $\mathfrak{g}$ *é dita* **semi-simples** *se* $\mathfrak{r} = 0$. *Ou seja,* $\mathfrak{g}$ *não possui ideais solúveis a não ser o ideal nulo.*

Proposição A.4.1 ([30]) *As seguintes condições são equivalentes:*

1. $\mathfrak{g}$ *é semi-simples;*
2. $\mathfrak{g}$ *é uma soma direta de álgebras de Lie simples (uma álgebra de Lie é dita* **simples** *quando não possui ideais não triviais e não é abeliana);*
3. *a forma de Cartan-Killing* $\langle\ ,\ \rangle_{CK}$ *de* $\mathfrak{g}$ *é não degenerada.*

Exemplo A.4.1 *Pode-se mostrar (por exemplo, calculando a forma de Cartan-Killing explicitamente) que as álgebras* $\mathfrak{gl}(n, I\!R)$, $\mathfrak{gl}(n,\mathbb{C})$ *e* $\mathfrak{u}(n)$ *são redutíveis mas não semi-simples. Já as álgebras* $\mathfrak{sl}(n, I\!R)$, $\mathfrak{sl}(n,\mathbb{C})$, $\mathfrak{su}(n)$ *e* $\mathfrak{so}(n)$ *são semi-simples.* □

Vale que uma álgebra de Lie real $\mathfrak{g}$ é semi-simples se, e somente se, sua complexificação $\mathfrak{g}^C$ também é semi-simples. De fato, a matriz da forma de Cartan-Killing relativa a uma base de $\mathfrak{g}$, é a mesma tanto para $\mathfrak{g}^C$ como para $\mathfrak{g}$. Ainda, se $\mathfrak{g}$ é simples então $\mathfrak{g}^C$ é também simples ou o produto de duas álgebras simples isomorfas. Se $\mathfrak{g}$ é semi-simples (resp. simples) então $\mathfrak{g}^R$ também o é. Uma subálgebra $\mathfrak{g}_0$ de $\mathfrak{g}^R$ é a *forma real* da álgebra de Lie complexa $\mathfrak{g}$ se $\mathfrak{g} = \mathfrak{g}_0 + \sqrt{-1}\mathfrak{g}_0$. As álgebras de Lie reais são formas reais ou realificações de álgebras de Lie complexas.

Definição A.4.3 *Seja $\mathfrak{g}$ uma álgebra de Lie semi-simples (real ou complexa). Dizemos que um elemento $X \in \mathfrak{g}$ é semi-simples se a transformação linear* $\mathrm{ad}(X) : \mathfrak{g} \longrightarrow \mathfrak{g}$ *é diagonalizável sobre $\mathbb{C}$. Uma* **subalgebra de Cartan** $\mathfrak{h} \subseteq \mathfrak{g}$ *é qualquer subálgebra maximal abeliana de $\mathfrak{g}$ consistindo de elementos semi-simples.*

A importância fundamental das subálgebras de Cartan no estudo da estrutura das álgebras de Lie complexas está no fato de que elas são conjugadas sob a ação adjunta do grupo $Int(\mathfrak{g})$, dos automorfismos internos de $\mathfrak{g}$. Isto não é verdade em geral para álgebras de Lie semi-simples reais, e esta é uma das razões que torna a estrutura de sua teoria mais complicada.

Daqui em diante, $\mathfrak{g}$ denotará uma álgebra de Lie semi-simples complexa. Como todas as subálgebras de Cartan de $\mathfrak{g}$ são conjugadas, não há perda de generalidade em escolhermos apenas uma, digamos $\mathfrak{h}$. Como $\mathfrak{h}$ é abeliana e o corpo de escalares $\mathbb{C}$ é algebricamente fechado, a representação adjunta ad de $\mathfrak{g}$, restrita a $\mathfrak{h}$, pode ser escrita como uma soma direta de representações unidimensionais. Em outras palavras, se $\mathfrak{h}^*$ denota o dual de $\mathfrak{h}$, e também para cada $\alpha \in \mathfrak{h}^*$, $\mathfrak{g}_\alpha$ denota o subespaço de todos os elementos $X \in \mathfrak{g}$ tais que $\mathrm{ad}(H)(X) = \alpha(H)X,\ \forall H \in \mathfrak{h}$, então $\mathfrak{g}$ é a soma direta dos $\mathfrak{g}_\alpha$. Dois destes subespaços $\mathfrak{g}_\alpha$ e $\mathfrak{g}_\beta$ são ortogonais com respeito a forma de Cartan-Killing a menos que $\alpha + \beta = 0$. Além disso $\mathfrak{g}_0 = \mathfrak{h}$, pois $\mathfrak{h}$ é seu próprio centralizador em $\mathfrak{g}$. Segue que $\mathfrak{h}$ é ortogonal a todos os $\mathfrak{g}_\alpha$, $\alpha \neq 0$, e portanto, a restrição da forma de Cartan-Killing à $\mathfrak{h}$ permanece não degenerada.

Como $\mathfrak{g}$ tem dimensão finita, apenas um número finito dos $\mathfrak{g}_\alpha$ é diferente do espaço nulo.

Definição A.4.4 *Se $\alpha \neq 0$ e $\mathfrak{g}_\alpha \neq \{0\}$, dizemos que α é uma* **raíz** *do par $(\mathfrak{g}, \mathfrak{h})$ e*

$$\mathfrak{g}_\alpha := \{X \in \mathfrak{g} : \mathrm{ad}(H)(X) = \alpha(H)X,\ \forall H \in \mathfrak{h}\}$$

o **espaço de raíz** *relacionado a α.*

Se α é uma raiz então $-\alpha$ também o é, pois caso contrário, $\mathfrak{g}_\alpha$ seria ortogonal a todo $\mathfrak{g}$, contrariando o fato de que a forma Cartan-Killing é não degenerada. Claramente, para cada raiz α vale $\dim(\mathfrak{g}_\alpha) = 1$. A justificativa para a terminologia vem da observação de que, se H é um elemento qualquer de $\mathfrak{h}$, os números complexos $\alpha(H)$ são os autovalores não nulos da transformação linear $\mathrm{ad}(H)$. Isto é, são as raízes não

nulas do polinômio característico

$$\det(\lambda - \mathrm{ad}(H)) = 0.$$

Denotamos por Π ou $\Pi(\mathfrak{g}, \mathfrak{h})$ o conjunto de todas as raízes do par $(\mathfrak{g}, \mathfrak{h})$. Trata-se de um subconjunto finito de $\mathfrak{h}^*$. Obtemos então uma decomposição em soma direta

$$\mathfrak{g} = \mathfrak{h} \oplus \sum_{\alpha \in \Pi} \mathfrak{g}_\alpha. \tag{A.21}$$

As raízes geram um subespaço real V de dimensão k de $\mathfrak{h}^*$, de modo que $V^c = \mathfrak{h}^*$. Tendo observado que a forma de Cartan-Killing de $\mathfrak{g}$ permanece não degenerada quando restrita à $\mathfrak{h}$, definimos um isomorfismo $\lambda \longmapsto H_\lambda$ de $\mathfrak{h}^*$ em $\mathfrak{h}$, e uma forma bilinear

$$\langle \lambda, \mu \rangle = \langle H_\lambda, H_\mu \rangle_{CK}$$

em $\mathfrak{h}^*$. Como a restrição de $\langle\ ,\ \rangle_{CK}$ à V toma valores reais e é positiva-definida, V adquire uma estrutura de espaço Euclidiano. Se $\mathfrak{h}_\Pi$ denota o espaço vetorial real gerado pelos H_α, $\alpha \in \Pi$, vale que $\mathfrak{h}$ é a complexificação de $\mathfrak{h}_\Pi$ e V o dual $\mathfrak{h}_\Pi^*$. Desse modo, construímos a partir de $\mathfrak{g}$ um conjunto finito Π de vetores não nulos no espaço Euclidiano V.

Definição A.4.5 *O conjunto* Π *obtido a partir das considerações acima é chamado* **sistema de raízes** *de* $\mathfrak{g}$. *De fato, a menos de isomorfismo, ele é independente da escolha da subalgebra de Cartan* $\mathfrak{h}$.

Em um certo senso intuitivo, podemos dizer que o conjunto acima representa o "esqueleto" de $\mathfrak{g}$. Ele é de fundamental importância, pois determina completamente a álgebra $\mathfrak{g}$ a menos de isomorfismo.

Teorema A.4.1 ([30]) *Nas condições acima, sejam* $\mathfrak{g}'$ *uma álgebra de Lie semi-simples,* $\mathfrak{h}'$ *uma subálgebra de Cartan de* $\mathfrak{g}'$ *e* Π' *o sistema de raízes do par* $(\mathfrak{g}', \mathfrak{h}')$. *Se existe um isomorfismo* $\phi : \mathfrak{h} \longrightarrow \mathfrak{h}'$ *que induz uma bijeção de* Π *em* Π', *então* ϕ *pode ser estendido a um isomorfismo* $\Phi : \mathfrak{g} \longrightarrow \mathfrak{g}'$.

Exemplo A.4.2 (A Álgebra Especial Linear) *Considere a álgebra de Lie semi-simples*

$$\mathfrak{sl}(n,\mathbb{C}) = \{A \in \mathfrak{gl}(n,\mathbb{C}) : \mathrm{tr}(A) = 0\},$$

e a subálgebra de Cartan $\mathfrak{h}$, formada por todas as matrizes diagonais com traço nulo. Tome E_{ij}, $1 \leq i, j \leq n$, a base canônica de $\mathfrak{gl}(n,\mathbb{C})$ e $\epsilon_i : \mathfrak{h} \longrightarrow \mathbb{C}$, $1 \leq i \leq n$, o funcional linear que associa a cada matriz seu i-ésimo elemento diagonal. Um cálculo direto mostra que, para cada $H \in \mathfrak{h}$, vale a igualdade

$$[H, E_{ij}] = (\epsilon_i - \epsilon_j)(H)E_{ij},$$

e desse modo os funcionais $\epsilon_i - \epsilon_j$ são raízes do par $(\mathfrak{sl}(n,\mathbb{C}), \mathfrak{h})$, quando $i \neq j$. Como claramente vale

$$\mathfrak{sl}(n,\mathbb{C}) = \mathfrak{h} \oplus \sum_{i \neq j} \mathrm{span}_C\{E_{ij}\}$$

essas são todas as raízes. O espaço real V gerado pelas raízes tem dimensão $n-1$. De fato, note que as raízes da forma $\epsilon_i - \epsilon_{i+1}$, $1 \leq i \leq n-1$, formam uma base de V. $\square$

Para cada raiz $\alpha \in \Pi$, tome $w_\alpha : V \longrightarrow V$ a reflexão no hiperplano V_α ortogonal a α. O sistema de raízes Π tem as seguintes propriedades [30]:

- $w_\alpha(\Pi) = \Pi, \ \forall \alpha \in \Pi$;
- $\langle \alpha^V, \beta \rangle \in \mathbb{Z}, \ \forall \alpha, \beta \in \Pi$; (onde $\alpha^V = 2\alpha/\langle \alpha, \alpha \rangle$)
- se $\alpha, \beta \in \Pi$ são proporcionais, então $\beta = \pm\alpha$.

Como não há espaço aqui para demonstrarmos todas as afirmações acima, vamos justificar brevemente o segundo item. Para cada par de raízes $\pm\alpha$ podemos escolher vetores $X_{\pm\alpha} \in \mathfrak{g}_{\pm\alpha}$ tais que $[X_\alpha, X_{-\alpha}] = H_{\alpha^V}$, a imagem de α^V pelo isomorfismo $\mathfrak{h}^* \simeq \mathfrak{h}$ induzido pela forma Cartan-Killing. O espaço vetorial $\mathfrak{s}_\alpha$ gerado por X_α, $X_{-\alpha}$ e H_{α^V} é uma subálgebra de Lie de $\mathfrak{g}$. A aplicação que leva estes três vetores respectivamente às matrizes

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \ \text{e} \ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

é um isomorfismo de $\mathfrak{s}_\alpha$ em $\mathfrak{sl}(2,\mathbb{C})$. Como em qualquer representação ρ de $\mathfrak{sl}(2,\mathbb{C})$ os autovalores de

$$\rho \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

são números inteiros, segue que $\langle \alpha^V, \beta \rangle \in \mathbb{Z}$. De fato, $\langle \alpha^V, \beta \rangle = \beta(H_{\alpha^V})$ é um

autovalor de $ad(H_{\alpha^V})$. O estudo das representações de $\mathfrak{sl}(2,\mathbb{C})$ obtidas restringindo ad as álgebras tridimensionais $\mathfrak{s}_\alpha$ é o método para a prova dos resultados acima.

Definição A.4.6 *O grupo W gerado pelas reflexões w_α é chamado* **grupo de Weyl** *(de Π ou de $\mathfrak{g}$). Os hiperplanos V_α dividem V em um número finito de componentes abertas conexas congruentes, denominadas* **câmaras de Weyl**.

O grupo de Weyl se comporta como um grupo de permutações das raízes $\alpha \in \Pi$, portanto trata-se de um grupo finito. Uma propriedade fundamental de Π é que o grupo de Weyl permuta as câmaras livre e transitivamente: isto é, se escolhemos uma câmara C, então qualquer outra câmara é da forma wC para um único elemento $w \in W$. Cada câmara C é limitada por k=dim(V) hiperplanos $V_{\alpha_i} = V_{-\alpha_i}$, $1 \leq i \leq k$. Uma das raízes do par $\pm\alpha_i$, digamos α_i, é tal que $\langle \alpha_i, x\rangle > 0$, para todo $x \in C$; o conjunto destas raízes é chamado de *base* de Π, ou *sistema simples de raízes*. De fato, toda raiz é uma combinação linear de um número finito de raízes simples, com coeficientes inteiros, todos positivos ou todos negativos. A partir destes coeficientes podemos introduzir uma ordem (a ordem lexicográfica) no conjunto de raízes, dividindo-o em duas componentes $\Pi = \Pi^+ \cup \Pi^-$, chamadas raízes *positivas* e *negativas*, respectivamente.

Exemplo A.4.3 *Se $\mathfrak{g} = \mathfrak{sl}(n,\mathbb{C})$ podemos considerar o sistema simples de raízes formado pelos elementos*

$$\alpha_i = \epsilon_i - \epsilon_{i+1},\ i = 1, ..., n-1$$

com a notação do exemplo anterior. A reflexão w_α correspondente a raiz $\alpha_i = \epsilon_i - \epsilon_j$ leva ϵ_i em ϵ_j e mantém todos os outros ϵ_k fixos. Disso, segue que W é isomorfo ao grupo de permutações de n elementos S_n. □

Definição A.4.7 *Uma álgebra de Lie real é dita* **compacta** *se sua forma de Cartan-Killing é negativa definida.*

Claramente, as álgebras compactas são semi-simples, pois sendo negativas definidas, suas formas de Cartan-Killing são não degeneradas. O próximo teorema fornece o significado topológico da definição acima.

Teorema A.4.2 *Uma álgebra de Lie real $\mathfrak{g}$ é a álgebra de Lie de um grupo de Lie compacto se, e somente se, $\mathfrak{g}$ é compacta.*

Um fato bastante importante, inclusive para mostrar o teorema posterior, é que dado um par $(\mathfrak{g}, \mathfrak{h})$ formado por uma álgebra de Lie complexa e uma subálgebra de Cartan, então ele admite uma base de Weyl. Se Π denota o conjunto de raízes de $(\mathfrak{g}, \mathfrak{h})$ e $\Sigma \subseteq \Pi$ é um sistema simples de raízes, então uma base de Weyl de $(\mathfrak{g}, \mathfrak{h})$ é uma base de $\mathfrak{g}$ formada pelos vetores $H_\alpha,\ \alpha \in \Sigma$; $X_\alpha \in \mathfrak{g}_\alpha,\ \alpha \in \Pi$ e satisfazendo

- $\langle X_\alpha, X_{-\alpha} \rangle_{CK} \ = \ 1$;
- $[X_\alpha, X_{-\beta}] \ = \ m_{\alpha\beta} X_{\alpha+\beta}$, com $m_{\alpha\beta} \in I\!R$ e tal que

$$m_{\alpha\beta} \ = \ -m_{-\alpha-\beta} \qquad \text{e} \qquad m_{\alpha\beta} \ = \ 0, \text{ quando } \alpha + \beta \notin \ \Pi.$$

Teorema A.4.3 ([30]) *Toda álgebra de Lie complexa $\mathfrak{g}$ admite formas reais compactas, isto é, subálgebras reais compactas. Se $\mathfrak{u}_1$ e $\mathfrak{u}_2$ são formas reais compactas de $\mathfrak{g}$, então existe um automorfismo ψ de $\mathfrak{g}$ tal que $\psi(\mathfrak{u}_1) = \mathfrak{u}_2$. Assim, todas as formas reais compactas de $\mathfrak{g}$ são isomorfas entre si.*

Referências Bibliográficas

[1] ALEKSEEVSKY D., *Isotropy Representation of Flag Manifolds*, Rend. Circ. Mat. Palermo (2) Suppl. 54, pp. 13-24, 1998.

[2] BACHOC C., BEN-HAIM Y., LITSYN S.; *Bounds for Codes in Products of Spaces, Grassmann, and Stiefel Manifolds*, IEEE Trans. Inf. Theory, vol. 54, no. 3, pp. 1024-1035, 2008.

[3] BARG A., NOGIN D. Y.; *Bounds on Packing of Spheres in the Grassmann Manifold*, IEEE Trans. Inf. Theory, vol. 48, no. 9, pp. 2450-2454, 2002.

[4] BORDEMANN M., FORGER M., ROMER H.; *Homogeneous Kähler manifolds: Paving the way towards supersymmetric sigma-models*, Comm. Math. Physics, vol. 102, pp. 605-647, 1986.

[5] BRESSAN J. P., COSTA S. I. R., GRAMA, L. A.; *Sphere Packing Bounds in Geometric Flag Manifolds*, submetido para publicação, IEEE Trans. Inf. Theory.

[6] CHEEGER J., EBIN D. G.; *Comparison Theorems in Riemannian Geometry*, North-Holland Publishing Company, 1975.

[7] CHOW W. L., *On the Geometry of Algebraic Homogeneous Spaces*, Annals. Math. 50, pp. 32-67, 1949.

[8] CONWAY J. H., HARDIN R. H., SLOANE N. J. A.; *Packing Lines, Planes, etc.: Packings in Grassmann Spaces*, Experimental Mathematics, vol. 5, no. 2, pp. 140-159, 1996.

[9] CARMO, M. P. do; *Geometria Riemanniana*, Coleção Projeto Euclides, Ed. IMPA, 2008.

[10] COSTA S. I. R., LAVOR C. C., ALVES M. M. S., SIQUEIRA, R. M.; *Uma Introdução à Teoria de Códigos*, ed. SBMAC, 2006.

[11] DAI W., LIU Y., RIDER B.; *Quantization Bounds on Grassmann Manifolds and Applications to MIMO Communications*, IEEE Trans. Information Theory, vol. 54, no. 3, pp. 1108-1123, 2007.

[12] ERICSON T., ZINOVIEV V.; *Codes on Euclidean Spheres*, North-Holland Mathematical Library, 2001.

[13] FOSCHINI G., GANS M.; *On Limits of Wireless Communications in Fading Environment when using Multiple Antenas*, Wireless Personal Commun., vol. 6, pp. 311-335, 1998.

[14] GALLOT S., HULIN D., LAFONTAINE J.; *Riemannian Geometry*, 2a. ed. Berlin, Germany: Springer, 1993.

[15] GHORPADE S., TSFASMAN M.; *Classical Varieties, Codes and Combinatorics*, Formal Power Series and Algebraic Combinatorics, pp. 75-84, Sweden, 2003.

[16] GRIFFITHS P., HARRIS J., *Principles os Algebraic Geometry*, Wiley, New York, 1978.

[17] GUANGYUE, H.; *Space Time Coding with Multiple Antenna Systems*, Tese de Doutorado, Universidade de Notre Dame, 2004.

[18] HENKEL O.; *Sphere-Packing Bounds in the Grassmann and Stiefel Manifolds*, IEEE Trans. Inf. Theory, vol. 51, no. 10, pp. 3445-3456, 2005.

[19] HERSTEIN I. N.; *Topics in Algebra*, Xerox College Publishing, 1964.

[20] HOCHWALD B., MARZETTA T.; *Unitary Space-time Modulation for Multiple-antenna Communications in Rayleigh Flat-fading Environment*, IEEE Trans. Inform. Theory, vol. 46, pp. 543-565, Mar. 2000.

[21] HUMPRHEYS, J. E.; *Introduction to Lie Algebras and Representation Theory*, Second printing, revised. Graduate Texts in Mathematics, Springer-Verlag, 1978.

[22] ITOH M.; *Curvature Properties of Kähler C-spaces*, J. Math. Soc. Japan, no. 30, pp. 39-71, 1978.

[23] KAMMOUN I., CIPRIANO A. M., BELFIORE J.; *Non-Coherent Codes over the Grassmannian*, IEEE Trans. Wireless Comm., vol. 6, no. 10, pp. 3657-3667, 2007.

[24] KOBAYASHI S., NOMIZU K.; *Foundations of Differential Geometry*, vols. I e II, Interscience Publishers, 1969.

[25] McWILLIAMS, F. J.; SLOANE, N. J. A.; *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, 1996.

[26] PITAVAL R., TIRKKONEN O., BLOSTEIN S. D.; *Density and Bounds for Grassmannian Codes with Chordal Distance*, 2011 IEEE Int. Symp. on Information Theory Proceedings, pp. 2298-2302.

[27] PUTTMANN T.; *Injectivity Radius and Diameter of the Manifolds of Flags in the Projective Planes*, Mathematische Zeitschrift, no. 246, pp. 795-809, 2004.

[28] RODIER F.; *Codes from Flag Varieties over a Finite Field*, Journal of Pure and Applied Algebra, no. 178, pp. 203-214, 2003.

[29] SAN MARTIN L. A. B.; *Notas de aula de Grupos de Lie*, http://www.ime.unicamp.br/smartin/cursos/grupolie-2006, IMECC, Campinas, 2006.

[30] SAN MARTIN L. A. B.; *Álgebras de Lie*, ed. Unicamp, Campinas, 1999.

[31] SOLÉ P., BELFIORE J.; *Constructive Spherical Codes Near the Shannon Bound*, Des. Codes and Cryptogr., 2012.

[32] TOREZZAN, C.; *Códigos Esféricos em Toros Planares*, Tese de Doutorado, IMECC - UNICAMP, 2009.

[33] WONG Y.; *Differential Geometry of Grassmann Manifolds*, Proc. Nat. Acad. Sci. USA, no. 57, pp.589-594, 1967.

[34] ZANELLA C., *Embeddings of Grassmann Spaces*, J. Geometry no. 52, pp. 193-201, 1995.

[35] ZHENG L., TSE D. N. C.; *Communication on the Grassmann Manifold: A geometric approach to the noncoherent miltiple-antenna channel*, IEEE Trans. Inf. Theory, vol. 48, no. 2, pp. 359-383, 2002.