UNIVERSIDADE ESTADUAL DE CAMPINAS

Faculdade de Engenharia Elétrica e de Computação

Leandro Bezerra de Lima

Contribuições em codificação no espaço projetivo e proposta de códigos quânticos de subespaços na grassmanniana

Campinas

2017

Leandro Bezerra de Lima

Contribuições em codificação no espaço projetivo e proposta de códigos quânticos de subespaços na grassmanniana

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

Orientador: Prof. Dr. Reginaldo Palazzo Júnior

Este exemplar corresponde à versão final da tese defendida pelo aluno Leandro Bezerra de Lima, e orientada pelo Prof. Dr. Reginaldo Palazzo Júnior

---

Campinas

2017

Agência(s) de fomento e nº(s) de processo(s): Não se aplica.
ORCID: http://orcid.org/0000-0002-7128-0789

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca da Área de Engenharia e Arquitetura
Rose Meire da Silva - CRB 8/5974

Lima, Leandro Bezerra de, 1979-
L628c Contribuições em codificação no espaço projetivo e proposta de códigos quânticos de subespaços na grassmanniana / Leandro Bezerra de Lima. – Campinas, SP : [s.n.], 2017.

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

1. Teoria da codificação. 2. Geometria hiperbólica. 3. Códigos corretores de erros (Teoria da informação). 4. Mecânica quântica. 5. Grasssmann, Variedades de. I. Palazzo Júnior, Reginaldo,1951-. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Contributions in coding over the projective space and proposal of quantum subspace codes in the Grassmannian
Palavras-chave em inglês:
Coding theory
Hyperbolic geometry
Error Correcting Codes (Information Theory)
Quantum mechanics
Grasssmann, Varieties
Área de concentração: Telecomunicações e Telemática
Titulação: Doutor em Engenharia Elétrica
Banca examinadora:
Reginaldo Palazzo Júnior
Antonio Aparecido de Andrade
Henrique Lazari
Wanessa Carla Gazzoni
Carlos Eduardo Câmara
Data de defesa: 06-06-2017
Programa de Pós-Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE DOUTORADO

Candidato: Leandro Bezerra de Lima
R.A.: 066557

Data da Defesa: 06 de Junho de 2017

Título da Tese: Contribuições em codificação no espaço projetivo e proposta de códigos quânticos de subespaços na grassmanniana

Prof. Dr. Reginaldo Palazzo Junior (Presidente, FEEC/UNICAMP/Campinas-SP)
Prof. Dr. Antonio Aparecido de Andrade (IBILCE/UNESP/São José do Rio Preto-SP)
Prof. Dr. Henrique Lazari (IGCE/UNESP/Rio Claro-SP)
Prof. Dr. Carlos Eduardo Câmara (UNIANCHIETA/Jundiaí-SP)
Profa. Dra. Wanessa Carla Gazzoni (UNISAL/Campinas-SP)

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

À minha querida esposa Patrícia pelo apoio, compreensão, carinho e amor;

Aos meus queridos filhos, Ana Clara, Ligia e Lucas. Amo Vocês!;

À todas as pessoas que contribuíram na minha formação
como pessoa, professor e pesquisador;

Dedico.

Agradecimentos

Agradeço a **Deus**, pela *Saúde*, *Paz* e *Harmonia*. Por propiciar ambiente para que pudesse concluir mais essa etapa.

Agradeço ao meu coração, minha amiga e esposa Patrícia pela oportunidade de passarmos parte de nossas vidas experimentando, vivenciando, curtindo momentos agradáveis e desafiosos juntos.

Agradeço aos meus lindos filhos, Ana Clara, Ligia e Lucas, pela oportunidade de me enxergar em vocês e por me fazerem feliz a cada dia.

Agradeço ao meu professor, orientador Prof. Dr. Reginaldo Palazzo Junior, por ter acreditado e apoiado de maneira incondicional a realização desse trabalho, contribuindo de forma ímpar para o meu desenvolvimento pessoal e acadêmico. Obrigado pelos momentos agradáveis de convivência com reuniões sempre produtivas rodeadas de incentivo, entusiasmo e confiança. Obrigado por tudo!.

Agradeço aos professores Prof. Dr. Antonio Aparecido de Andrade - IBILCE/UNESP, Prof. Dr. Henrique Lazari - IGCE/UNESP, Prof. Dr. Carlos Eduardo Câmara - UNIANCHIETA, Profa. Dra. Wanessa Carla Gazzoni - UNISAL, Prof. Dr. Cristiano Torezzan - FCA/UNICAMP, Prof. Dr. Renato da Rocha Lopes - FEEC/UNICAMP e o Prof. Dr. Agnaldo José Ferrari - FC/UNESP, por aceitarem participar da banca de defesa.

Agradeço a todos os professores do doutorado em Engenharia Elétrica - (FEEC/UNICAMP), em especial, Palazzo, Max Costa, José Cândido, (IMECC/UNICAMP) Fernando Torres, Marcelo Firer, (FCA-UNICAMP) Cristiano Torezzan e (FT-UNICAMP) Profª. Drª. Marli de Freitas Gomes Hernandez.

Agradeço a todos os amigos da pós graduação, pelos momentos agradáveis de convivência e aprendizagem, tanto no LTIA quanto em outros ambientes, Gustavo, Mário, Anderson, Luiz Leandro, Nelson, Akemi, Ángela, Cintya, Luzinete, Cibele, Maicon, Fernando, Lucas, Tiago e Diogo.

Agradeço a todos os professores e colegas do projeto temático FAPESP, pelos diversos momentos de aprendizado proporcionado.

Aos funcionários da pós-graduação FEEC-UNICAMP por ser muito atenciosos e por sempre realizar um trabalho de altíssima qualidade.

Agradeço a todos que compõem minha grande FAMÍLIA e contribuiram para o

sucesso dessa etapa, aos meus pais José e Joana, aos meus sogro e sogra Jaime e Evelise, a minhas irmãs Alessandra, Karen e Karina, cunhados Adeilton, Everson e Guilherme, cunhadas Priscila, Giordanna e Gislene, sobrinhos e sobrinhas Ana Luisa, Luiza, Nicolas e Theo, tios, tias, primos e primas Paulo e Simone, Antonio e Cida, Tulu e Marli, Arlene, Elenice, Tunico, Renata, Mauro, Michele meus avôs e avós in memorian José Carmindo e Cidalina, José Bezerra e Antônia e amigos especiais João Batista e Elisabete, Edvaldo, Giovanna e Gabriel.

Agradeço aos colegas e amigos do Campus de Aquidauana - CPAQ da Universidade Federal de Mato Grosso do Sul - UFMS, em especial, aos amigos da Matemática, João Batista, Adriana, César, Denise, Irene e aos amigos do Campus, Edvaldo, Firmino, Auri, Edna, Miguel, Maria Helena, Alice, Ana Paula, Carlos Martins, entre outros. Obrigado pela convivência, oportunidade de aprendizado e de me qualificar.

Agradeço aos meus diversos alunos que hoje em dia já são meus colegas de profissão pelo desafio de proporcionar um caminho a trilhar, em especial, Elizeu França, Augusto, Thales, Juliana, Renan, Camila e Ana Paula, entre outros.

"Os primeiros passos em qualquer ramo da pesquisa quase sempre são muito imperfeitos e não raro terminam em fracasso. As verdades ás vezes são como os recantos mais inacessíveis de alguma localidade, cuja descoberta do acesso exige que tenhamos todos caminhos possíveis. Cumpre porém que um certo número de pessoas se disponha a correr os riscos que a busca envolve a fim de deixar os rastros desses caminhos....A busca da verdade é indissociável das experiências frustradas."

*(**Denis Diderot**).*

"Não conseguimos encontrar respostas para todos os nossos problemas. As que encontramos apenas nos levaram a formular novas questões. Dê uma certa maneira sentimo-nos tão confusos como antes, mas acreditamos que agora estamos confusos num nível mais alto e sobre coisas mais importantes."

*(**Aviso na porta do Instituto de Matemática da Universidade de Tronso - Noruega**).*

"Uma teoria matemática não será considerada completa até que você a tenha feito tão clara que seja possível explicá-la para o primeiro homem que você encontrar na rua"

*(**David Hilbert**).*

"Aprendei a conduzir vossa imaginação e a vida vos será mais fácil."

*(**Ruy Madsen Barbosa**).*

"10% de genialidade e 90% de transpiração"

*(**Albert Einstein**).*

Resumo

Este trabalho de doutorado consiste em apresentar algumas contribuições em codificação no espaço projetivo. Esta é uma área de pesquisa que possui importantes aplicações em codificação de rede. A conexão entre codificação no espaço projetivo e a codificação de rede se dá através do canal de comunicação matricial. Neste contexto, mostramos um estudo de códigos de subespaços n-shot geometricamente uniforme, trazendo uma construção de tais códigos. Evidenciamos um isomorfismo entre reticulado de um grupo abeliano consistindo do grupo das unidades do corpo finito $\mathbb{F}_p$, p primo, e o diagrama de Hasse de espaços projetivos $\mathbb{P}(\mathbb{F}_p^m)$. Esse isomorfismo permite trabalhar em ambas as estruturas, os códigos de subespaços n-shot. Por fim, exibimos uma proposta de construção de códigos quânticos de subespaços na grassmanniana. Neste caso, uma possibilidade é a aplicação em codificação de redes quânticas. Dado isso, propomos duas construções de códigos quânticos de subespaços na grassmanniana. A primeira, descrevemos um rotulamento do estado quântico separável arbitrário universal, e a partir desse rotulamento, associamos a códigos de subespaços na grassmanniana, com a máxima distância de subespaços, estados quânticos com o máximo emaranhamento global, também usamos os códigos de subespaços n-shot para descrever estados quânticos de máximo emaranhamento global generalizado. E a segunda, exibimos um rotulamento associado diretamente à uma classe de estados quânticos de máximo emaranhamento global por meio de uma matriz modificada da classe dos códigos Reed-Muller.

Palavras-chaves: Codificação no Espaço Projetivo; Códigos de Subespaços n-shot Geometricamente Uniforme, Design Combinatório; Reticulado de Grupo; Códigos Quânticos de Subespaços.

Abstract

This doctoral thesis consists on the introduction of some contributions for the projective space codification. This is an area with important applications on Network coding. The connection between codification on the projective space and network coding rises through the matrix communication channel. In this context, we present a study of geometrically uniform n-shot subspace codes, and a construction for such codes. We make evident an isomorphism between an Abelian group lattice, consisting on the unit group of the field $\mathbb{F}_p$, p is a prime number, with the Hasse diagram of projective spaces $\mathbb{P}(\mathbb{F}_p^m)$. This isomorphism allows to work in both structures, the n-shot subspace codes. In this case, one possibility is the application on the codification of quantum networks. Given that, we propose two proposals for the construction of subspace quantum codes in the Grassmannian. The first, we describe a labeling of the universal arbitrary and separable quantum state, and from this labeling, we associate subspace codes in the Grassmannian, with the maximum subspace distance, to quantum states with the maximum global entanglement, we also use the n-shot subspaces codes to describe quantum states of maximum generalized global entanglement. And the second, we exhibit a labeling directly associated to a class of quantum states of maximum global entanglement through a modified matrix from the class of Reed-Muller codes.

Keywords: Coding in Projective Space; Geometrically Uniform n-shot Subspace Codes; Combinatorial Design; Group Lattice; Quantum Subspace Codes.

Lista de Figuras

Lista de Tabelas

Lista de Acrônimos e Notação

$\mathbb{N}$	Conjunto dos números naturais.
$\mathbb{Z}$	Conjunto dos números inteiros.
$\mathbb{Z}_n$	Conjunto dos números inteiros módulo n.
$\mathbb{R}$	Conjunto dos números reais.
$\mathbb{F}_q$	Corpo finito com q elementos.
$(G, *)$	Grupo.
G/H	Grupo quociente do grupo G pelo subgrupo H.
$H \lhd G$	H é um subgrupo normal do grupo G.
$\|G\|$	Ordem do grupo G.
Hx	Classe lateral à direita.
xH	Classe lateral à esquerda.
D_n	Grupo diedral ou grupo das simetrias de grau n.
S_n	Grupo de permutações ou grupo simétrico de grau n.
$R_V(s)$	Região de Voronoi associada a s.
$DP(s)$	Perfil distância global associado a um elemento $s \in S$.
U(S)	Grupo gerador do conjunto de sinais geometricamente uniforme S.
U'	Subgrupo normal de $U(S)$.
S/S'	Partição geometricamente uniforme.
$\mathbb{P}(\mathbb{F}_q^n)$	Espaço projetivo n-dimensional sob um corpo finito com q elementos.
$\mathcal{G}(\mathbb{F}_q^m, k)$	Grassmanniana de dimensão k.
z^*	Conjugado complexo de z.
$\|\psi\rangle$	Vetor, também chamado de Ket.
$\langle\psi\|$	Vetor dual de $\|\psi\rangle$, também chamado de Bra.

$\langle\varphi\|\psi\rangle$	Produto interno entre $\|\varphi\rangle$ e $\|\psi\rangle$.
$\|\varphi\rangle\langle\psi\|$	Produto externo entre $\|\varphi\rangle$ e $\|\psi\rangle$.
$\|\varphi\rangle \otimes \|\psi\rangle$	Produto tensorial entre $\|\varphi\rangle$ e $\|\psi\rangle$.
$\|\varphi\rangle \, \|\psi\rangle$	Notação abreviada para o produto tensorial entre $\|\varphi\rangle$ e $\|\psi\rangle$.
A^*	Conjugado complexo da matriz A.
$A^\top$	Transposta da matriz A.
$A^\dagger$	Conjugado hermitiano ou matriz adjunta de A.
$\langle\varphi\|A\|\psi\rangle$	Produto interno entre $\|\varphi\rangle$ e A$\|\psi\rangle$.

Sumário

1 Introdução Geral do Trabalho

1.1 Motivação

A codificação de rede (Network Coding, em Inglês) introduzida em (AHLSWEDE *et al.*, 2000) permite buscar melhor desempenho e eficiência na transmissão da informação a partir da estratégia de utilizar cada nó da rede como um processador digital da informação, ou seja, permite que se realize operações e processamento em cada nó e não mais apenas rotear, isto é, selecionar caminhos adequados para a informação trafegar na rede. Cabe ressaltar que roteamento é um caso particular de codificação de rede, dado que nas operações permitidas na codificação podemos apenas replicar e selecionar caminhos para a informação trafegar na rede. Como recurso de argumentação, em (AHLSWEDE *et al.*, 2000) a rede borboleta justifica a importância de permitir que nós da rede possam atuar como processador digital possibilitando ganhos em termos de taxa de transmissão. Na rede borboleta cada canal permite a transmissão de apenas um único bit por unidade de tempo, instantaneamente e sem erros e o objetivo é transmitir informação do nó fonte **F** para os nós destinos $\mathbf{D}_1$ e $\mathbf{D}_2$. Quando usamos apenas o roteamento nos nós da rede, o melhor que obtemos está ilustrado na Figura 1. Observe que no primeiro instante o nó $\mathbf{D}_1$ recebe apenas o bit a_1 já que o nó 3 selecionou enviar o bit a_1 e o nó $\mathbf{D}_2$ recebeu os bits a_1 e a_2. No instante seguinte o nó $\mathbf{D}_1$ recebe os bits a_2 e a_3 e o nó $\mathbf{D}_2$ recebe apenas o bit a_3. Neste processo, a taxa de informação é 1,5 bit por unidade de tempo, ou seja, 3 bits em dois instante de tempo.

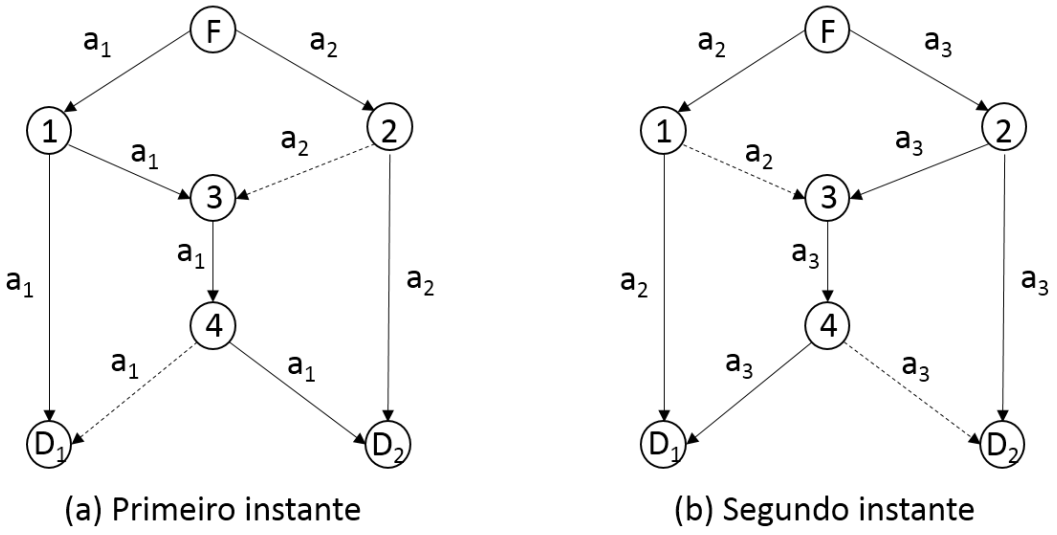


Figura 1 – Rede Borboleta Utilizando Roteamento

Quando permitimos que nós da rede funcionem como um processador digital ob-

temos um ganho de 0,5 bit por instante de tempo, pois é possível trasmitir 2 bits por instante de tempo, como ilustrado na Figura 2. Para isso, a operação nó 3 é a soma módulo 2 dos bits que recebe e transmite o resultado para o nó 4. Assim, tanto o nó $\mathbf{D}_1$ quanto o nó $\mathbf{D}_2$ recebem os bits a_1 e a_2, respectivamente, bastando ambos efetuarem uma soma módulo 2 para obter o correspondente bit.

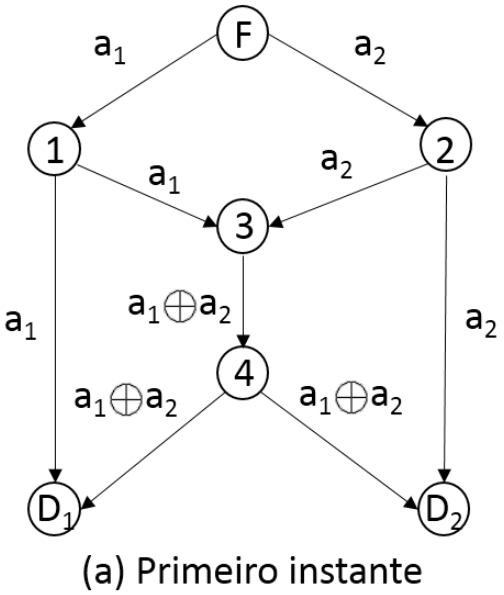


Figura 2 – Rede Borboleta Utilizando Codificação de Rede

Portanto, em se tratando de taxas de informação, existe um ganho, quando se permite que nós da rede funcionem como um processador digital, justificando a utilização de codificação de rede.

1.2 Descrição de Trabalhos Anteriores

No caso geral, não existe restrições nas operações efetuadas pelos nós da rede. Mas, no trabalho pioneiro de (LI *et al.*, 2003) mostra-se que é suficiente restringir as operações sobre os pacotes a combinações lineares, para o caso de um único nó fonte. No artigo (YEUNG; CAI, 2006), os autores propõem utilizar os códigos corretores de erros para o caso em questão, ou seja, de um único nó fonte. A ideia fundamental de controle de erros em codificação de rede, mesmo na presença de erros, é permitir que possa ser decodificada pelos nós destinos a informação gerada pelo nó fonte, com a distribuição de redundância pelos diversos canais. O canal de comunicação matricial, que modela a comunicação na presença de erros é mostrado na Figura 3, onde o nó fonte transmite a matriz X. O nó destino recebe a matriz $Y = GX + Z$, onde G representa o código de rede e Z representa os erros. Tanto o problema de controle de erros em redes, quanto o problema de codificação de rede não coerente podem ser estudados em conjunto por meio

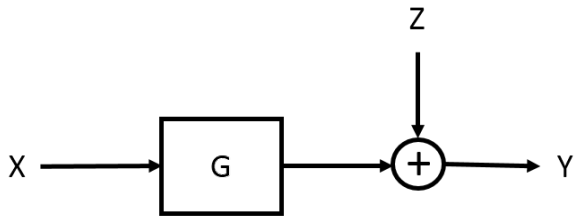


Figura 3 – Canal de Comunicação Matricial

do canal de comunicação matricial. Em (KöETTER; KSCHISCHANG, 2008) sob a ótica de considerar $Z = 0$, temos que cada pacote é um vetor com n elementos de um corpo finito $\mathbb{F}_q$. Portanto, pode-se modelar a comunicação entre um nó fonte e um nó destino da rede pela expressão:

$$Y = GX,$$

onde a mensagem transmitida pelo nó fonte é uma matriz $X \in \mathbb{F}_q^{s\times n}$ cujas linhas são representadas por $X_1, X_2, \cdots, X_s \in \mathbb{F}_q^{1\times n}$ e são os s pacotes de entrada na rede pelo nó fonte, $Y \in \mathbb{F}_q^{r\times n}$ é a matriz onde as linhas representadas por $Y_1, Y_2, \cdots, Y_r \in \mathbb{F}_q^{1\times n}$ são os r pacotes de saída na rede pelo nó destino e $G \in \mathbb{F}_q^{r\times s}$ é a chamada **matriz de tranferência** de X para Y. Cabe observar que as entradas dependem da topologia da rede e das combinações lineares realizadas pelos nós intermediários. Em (NóBREGA, 2013) faz-se um estudo sobre o canal matricial multiplicativo (MMC, do Inglês Multiplicative Matrix Channel) sobre corpos finitos, onde a matriz de transferência são desconhecidas tanto do transmissor quanto do receptor, esse caso é chamado **MMC não coerente**. Códigos para MMC não coerente são chamados de **códigos matriciais** e esses códigos estão associados aos **códigos de subespaços**.

Em (KöETTER; KSCHISCHANG, 2008) mostram-se que uma possibilidade eficiente para controle de erros em codificação de rede é utilizar códigos de subespaços, que são códigos construídos sobre o espaço projetivo. Uma outra alternativa é a utilização de design combinatório. Enquanto os códigos de subespaços evidenciam uma estrutura algébrica, o design combinatório é uma importante estrutura combinatória com alto grau de regularidade e que está relacionada a existência e construção de sistemas de conjuntos de cardinalidade finita (STINSON, 2004). Como exemplo, mencionamos a relação existente entre códigos corretores de erros em espaço de Hamming e design combinatório, onde as palavras-código de peso 3 do código de Hamming formam um sistema triplo de Steiner STS(7), um plano projetivo de ordem 2, conhecido como plano de Fano (ETZION; SILBERSTEIN, 2009), assim como q-analogs de um código de peso constante no espaço de Hamming é um código na grassmanniana do espaço projetivo, (BRAUN *et al.*, 2013; ETZION; VARDY, 2011). No contexto da mecânica quântica, o processamento de forma eficiente está fundamentado em estados quânticos emaranhados que satisfazem as condições de máximo emaranhamento global, segundo a medida de Meyer-Wallach.

1.3 Proposta de Trabalho

Propomos a definição do conceito de códigos de subespaços n-shot geometricamente uniforme e apresentamos uma construção de tais códigos, partindo da premissa de utilizar o canal de subespaço n-vezes. Também propomos um isomorfismo entre o reticulado de um grupo Abeliano consistindo do grupo das unidades do corpo finito $\mathbb{F}_p$ e o diagrama de Hasse de espaços projetivos $\mathbb{P}(\mathbb{F}_p^m)$, com intuito de fornecer uma altenartiva para tratar códigos de subespaços n-shot.

Além disso, apresentamos o estudo e a construção de códigos quânticos de subespaços na grassmanniana, por meio, de duas propostas de rotulamentos. Uma que descreve um estado quântico separável arbitrário universal e a partir desse rotulamento obtemos o código quântico de subespaço na grassmaniana associado a um estado de máximo emaranhamento global. E através dessa associação, obtemos novos estados quânticos de máximo emaranhamento global utilizando os códigos de subespaços n-shot. A outra proposta, associa códigos de subespaços na grassmanniana diretamente a estados de máximo emaranhamento global, proveniente de uma matriz modificada dos códigos Reed-Muller, dando origem ao código quântico de subespaço na grassmanniana.

1.4 Descrição do Trabalho

Este trabalho está organizado da seguinte forma. No Capítulo 2, apresentamos alguns conceitos que são necessários para a compreensão da trabalho. No Capítulo 3, apresentamos os primeiros resultados deste trabalho. Uma alternativa para obter códigos de subespaços com boas taxas e boas capacidades de correções de erros, sem a necessidade de aumentar o tamanho do corpo finito $\mathbb{F}_q$, ou do comprimento m do vetor, é utilizar o canal n-vezes, ou seja, codificar a informação em uma sequência de subespaços a ser enviada e não apenas em um único subespaço, a esse novo código dá-se o nome de códigos de subespaços n-shot (NóBREGA; UCHôA-FILHO, 2009). Com isso, apresentamos os conceitos de códigos de subespaços geometricamente uniforme, que são códigos com propriedades álgebricas e geométricas interessantes tanto do ponto de vista matemático quanto de comunicações, além de possuírem eficientes algoritmos associados ao processo de decodificação, apresentamos também uma classe de códigos de subespaços n-shot geometricamente uniforme por meio da utilização do canal n-vezes. No Capítulo 4, mostramos um isomorfismo entre o reticulado de um grupo Abeliano consistindo do produto direto do grupo das unidades do corpo $\mathbb{F}_p$ (grupo multiplicativo) e o diagrama de Hasse de espaços projetivos $\mathbb{P}(\mathbb{F}_p^m)$, cujo objetivo é fornecer elementos que possam ser úteis para elaboração e construção de códigos de subespaços. No Capítulo 5, apresentamos duas propostas de rotulamento de estados quânticos emaranhados, uma descrevendo um estado quântico puro separável e outra apartir de um estado puro de máximo emara-

nhamento global, além de apresentarmos por meio dos códigos de subespaços n-shot uma extensão de estados puros de máximo emaranhamento global (GAZZONI, 2008).

2 Conceitos Preliminares

Este capítulo revisa elementos considerados fundamentais para o embasamento e entendimento desta tese. Para maiores detalhes, sugerimos (DOMINGUES; IEZZI, 2003; MACWILLIAMS; SLOANE, 1983; STINSON, 2004; ROMAN, 2008; FORNEY, 1991; SLEPIAN, 1968)

2.1 Revisão de Estruturas Algébricas

2.1.1 Elementos sobre Grupos

Definição 2.1. *Uma* ***operação binária*** *"$*$" sobre um conjunto não vazio G é uma função que associa a cada par (a, b) de $G \times G$ um elemento de G, denotado por $a * b$, através da função $* : G \times G \to G$.*

Definição 2.2. *Um* ***grupo*** *é um par $(G, *)$ consistindo de um conjunto não vazio G e uma operação binária $* : G \times G \to G$ tal que, as seguintes propriedades são satisfeitas:*

1. *A operação $*$ é* ***associativa****, i.e, $(a * b) * c = a * (b * c)$, $\forall\ a, b, c \in G$.*
2. *Existe um* ***elemento neutro*** *"e" em G, tal que, $a * e = e * a = a$, $\forall\ a \in G$.*
3. *Para todo elemento de G existe* ***elemento inverso*** *com relação a operação $*$ em G, isto é, $\forall a \in G$, $\exists\ a^{-1}$ tal que $a * a^{-1} = e = a^{-1} * a$.*

   Se em $(G, *)$ valer uma propriedade adicional:

4. *A operação $*$ é* ***comutativa****, i.e, $(a * b) = (b * a)$ $\forall\ a, b \in G$*

Dizemos que $(G, *)$ é um ***grupo abeliano****.*

Em qualquer grupo, pode-se mostrar os seguintes fatos:

- O elemento identidade de um grupo G é único.
- O elemento inverso de um dado elemento é único.

Definição 2.3. *Se um subconjunto H de um grupo G é fechado sob a operação binária sobre G e se H é um grupo sob esta operação binária, então H é chamado* ***subgrupo*** *de G. Escreve-se $H \leq G$.*

Definição 2.4. *Seja G um grupo e seja $a \in G$. O conjunto*

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

é um subgrupo de G e é o menor subgrupo de G que contém a, ou seja, qualquer outro subgrupo que contém a contém também H e H é chamado ***subgrupo cíclico de*** *G* ***gerado por*** *a, e denota-se por $\langle a \rangle$.*

Definição 2.5. *Se $G = \langle a \rangle$, para algum $a \in G$ dizemos que G é um* ***grupo cíclico****.*

Definição 2.6. *Seja G um grupo. Se G possui um número finito de elementos, dizemos que G é um* ***grupo finito****. A* ***ordem*** *de G, denotada por $|G|$, o número de elementos de G.*

Definição 2.7. *A* ***ordem*** *n de um elemento a pertencente a um grupo G é o menor inteiro positivo tal que $a^n = e$, onde e é a identidade do grupo.*

Apresentamos, a seguir, exemplos importantes de grupos que são muito usados, por exemplo, no processo de modulação codificada.

Exemplo 2.1. *O* ***grupo diedral*** *ou* ***grupo de simetrias*** *D_n com $n \geq 3$, ou seja, o conjunto de simetrias de um polígono regular de n lados com a composição de simetrias.*

Exemplo 2.2. *O* ***grupo de permutações*** *ou* ***grupo simétrico de grau n*** *S_n, ou seja, $X = \{1, 2, \cdots, n\}$ o conjunto de todas as aplicações bijetivas de X em X com a composição de funções.*

Definição 2.8. *Sejam $H \leq G$ e $x \in G$. O subconjunto de G*

$$Hx = \{hx : h \in H\}$$

é chamado ***classe lateral a direita*** *de H em G. De maneira análoga se define* ***classe lateral a esquerda*** *de H em G. Quando o número de classes laterais (à esquerda ou à direita) for finito, o número de classes laterais é chamado de* ***índice*** *de H em G e denotado por $[G : H]$. Caso seja válido $xH = Hx$ para todo $x \in G$, dizemos que H é um* ***subrgrupo normal*** *de G e denotamos $H \lhd G$. Assim, podemos definir o* ***grupo quociente*** *de G pelo subgrupo normal H como sendo o conjunto $G/H = \{xH : x \in G\}$ munido da operação entre classes laterais $(xH) * (yH) := (x * y)H$.*

Observação 2.1. *Se G é um grupo abeliano, então todo subgrupo H de G é normal em G.*

Teorema 2.1. *(**Teorema de Lagrange**) Sejam G um grupo finito e H um subgrupo de G. Então $|G| = |H|[G : H]$, ou seja, o número de elementos de H e o índice de H em G dividem o número de elementos de G.*

Definição 2.9. *Considere dois grupos $(G, \cdot)$ e $(\hat{G}, *)$ e uma função $\phi : G \to \hat{G}$. Diz-se que ϕ é um* ***homomorfismo*** *de G em $\hat{G}$ se:*

$$\phi(a \cdot b) = \phi(a) * \phi(b)$$

para todo $a, b \in G$. (Note que a operação $a \cdot b$ ocorre em G, enquanto que a operação $\phi(a) * \phi(b)$ ocorre em $\hat{G}$).

Definição 2.10. *Um* ***isomorfismo de grupos*** *de G em $\hat{G}$ é um homomorfismo onde a função $\phi : G \to \hat{G}$ é bijetora. Neste caso, diz-se que G e $\hat{G}$ são isomorfos e denota-se: $G \cong \hat{G}$.*

Teorema 2.2. *(**Teorema de Cayley**) Se G é um grupo então ele é isomorfo a um subgrupo de S_G (grupo das bijeções de G). Em particular, se G tem ordem n então G é isomorfo a um subgrupo de S_n.*

2.1.2 Elementos sobre Corpos Finitos

Definição 2.11. *Um* ***corpo*** *$(K, +, \cdot)$ é um conjunto, denotado por K, com duas operações binárias ("$+$" e "$\cdot$"), tal que as seguintes propriedades são satisfeitas:*

1. *$(K, +)$ é um grupo abeliano, onde o elemento "0" representa o elemento identidade.*
2. *$(K^* := K \setminus \{0\}, \cdot)$ é um grupo abeliano, onde o elemento "1" representa o elemento identidade. Neste caso, K^* é composto por todos os elementos de K com exceção do zero (elemento identidade associativo).*
3. *A operação "$\cdot$" se distribui sobre "$+$", i.e, $a \cdot (b + c) = (a \cdot b) + (a \cdot c), \ \ \forall a, b, c \in K$*

Quando K for finito, dizemos que $(K, +, \cdot)$ é um ***corpo finito***

Observação 2.2. *Os corpos finitos também são chamados* ***corpos de Galois*** *e são denotados por $GF(q)$ ou $\mathbb{F}_q$ onde $q \geq 2$ é o número de elementos do corpo.*

Definição 2.12. *Um* ***subcorpo*** *é um subconjunto de um corpo que tem a estrutura de um corpo sob as operações herdadas do mesmo.*

2.1.3 Elementos sobre Espaços Vetoriais

Definição 2.13. *Sejam um corpo K, cujos elementos são chamados de* ***escalares****, e um conjunto não vazio V, cujos elementos são chamados de* ***vetores****. Dizemos que V é um* ***espaço vetorial*** *sobre o corpo K, ou é um K-**espaço vetorial**, sob a operação de adição em V,*

$$\begin{aligned} + : V \times V &\to V \\ (v, w) &\to v + w \end{aligned}$$

e sob a operação de multiplicação por escalar de elementos de V por elementos de K,

$$\begin{aligned} \cdot : K \times V &\to V \\ (\lambda, w) &\to \lambda v \end{aligned}$$

satisfazendo as seguintes propriedades:

1. $u + v = v + u, \quad \forall\ u, v \in V$ *(comutativa).*
2. $(u + v) + w = u + (v + w), \quad \forall\ u, v, w \in V$ *(associativa).*
3. *existe elemento neutro em V, denominado de vetor nulo e denotado por 0, tal que* $0 + u = u + 0 = u, \quad \forall\ u \in V$ *(elemento neutro).*
4. *existe elemento inverso em V, denominado simétrico de u e denotado por $-u$, tal que* $(-u) + u = u + (-u) = 0, \quad \forall\ u \in V$ *(elemento inverso).*
5. $(\alpha + \beta)u = \alpha u + \beta u$, *para todo α, β em K e u em V.*
6. $\alpha(u + v) = \alpha u + \alpha v$, *para todo α em K e u, v em V.*
7. $(\alpha\beta)u = \alpha(\beta u)$, *para todo α, β em K e u em V.*
8. $1u = u$, *para todo u em V,onde 1 é a unidade do corpo K.*

Exemplo 2.3. *Todo corpo K é um espaço vetorial sobre si mesmo.*

Exemplo 2.4. *K^n com $n \in \mathbb{N}$, é um espaço vetorial sobre K. Em particular, $\mathbb{F}_q^n$ com $n \in \mathbb{N}$, é um espaço vetorial sobre $\mathbb{F}_q$ e $\mathbb{Z}_2^n$ com $n \in \mathbb{N}$, é um espaço vetorial sobre $\mathbb{Z}_2$.*

Definição 2.14. *Considere um espaço vetorial V sobre um corpo K. Um subconjunto não vazio $U \subset V$ é um* ***subespaço vetorial*** *de V sobre K se U satisfaz as seguintes condições:*

1. $u + v \in U$, *para todo $u, v \in U$.*
2. $\alpha u \in U$, *para todo $\alpha \in K$ e $u \in U$.*

Exemplo 2.5. *Considere o espaço vetorial $\mathbb{Z}_2^3$ sobre o corpo $\mathbb{Z}_2$. O conjunto*

$$U = \{(0,0,0), (1,0,1), (1,0,0), (0,0,1)\} \subset \mathbb{Z}_2^3,$$

é um subespaço vetorial de $\mathbb{Z}_2^3$.

Definição 2.15. *Um vetor $v \in V$ é uma* ***combinação linear*** *dos vetores $v_1, v_2, \cdots, v_n \in V$ se existirem escalares $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$ tal que:*

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n.$$

Definição 2.16. *Sejam V um espaço vetorial sobre um corpo K e $v_1, v_2, \cdots, v_n \in V$. Dizemos que o conjunto de vetores $\{v_1, v_2, \cdots, v_n\}$ é* ***linearmente independente (LI)****, se a combinação linear*

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$$

implica em $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$, onde $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$.

Caso contrário, ou seja, exista algum $a_i \neq 0$ para algum i, dizemos que o conjunto de vetores $\{v_1, v_2, \cdots, v_n\}$ é ***linearmente dependente (LD)****.*

Definição 2.17. *Um espaço vetorial V sobre um corpo K tem* ***dimensão finita****, e é denotado por $dimV$, se existe um subconjunto finito de V cujos vetores geram V. Caso contrário, dizemos que V tem* ***dimensão infinita****.*

Definição 2.18. *Seja V um espaço vetorial sobre um corpo K. Um subconjunto $B \subset V$ é uma* ***base*** *de V se:*

1. *Se os elementos de B geram V;*
2. *Se os elementos de B forem linearmente independentes.*

Exemplo 2.6. *O conjunto das n-uplas sobre $\mathbb{F}_q$ forma um espaço vetorial de dimensão n, cuja base é $B = \{e_1 = (1, 0, 0, \cdots, 0), e_2 = (0, 1, 0, \cdots, 0), \cdots, e_n = (0, 0, 0, \cdots, 1)\}$.*

Definição 2.19. *Seja V um espaço vetorial sobre um corpo K. Um* ***produto interno*** *sobre V é uma função que a cada par (u, v) em $V \times V$ associa um escalar em K, denotado por $u \cdot v$ e satisfazendo as seguintes propriedades para todos u, v e $w \in V$ e $\alpha \in K$:*

1. *$u \cdot v \geq 0$ e $u \cdot u = 0$ se, e somente se, $u = 0$;*
2. *$u \cdot v = v \cdot u$;*
3. *$u \cdot (v + w) = u \cdot v + u \cdot w$;*
4. *$(\alpha u) \cdot v = \alpha(u \cdot v)$.*

Exemplo 2.7. *O produto interno de duas n-uplas $u = (u_1, u_2, \cdots, u_n)$ e $v = (v_1, v_2, \cdots, v_n)$ é o escalar:*

$$u \cdot v = u_1 v_1 + u_2 v_2 + \cdots + u_n v_n$$

Definição 2.20. *Dois vetores u e $v \in V$ são* ***ortogonais*** *se $u \cdot v = 0$.*

Exemplo 2.8. *Os vetores $u = (1, 0, 0)$ e $v = (0, 0, 1) \in \mathbb{Z}_2^3$ são ortogonais, pois*

$$u \cdot v = (1, 0, 0) \cdot (0, 0, 1) = 1 \cdot 0 + 0 \cdot 0 + 0 \cdot 1 = 0.$$

Já os vetores $u = (1, 0, 1)$ e $v = (0, 0, 1) \in \mathbb{Z}_2^3$ não são ortogonais, pois

$$u \cdot v = (1, 0, 1) \cdot (0, 0, 1) = 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 = 1 \neq 0.$$

Definição 2.21. *Sejam V um espaço vetorial e $U \subset V$ um subespaço vetorial de V. Definimos por $U^{\perp}$ o subconjunto formado pelos vetores de V que são ortogonais a todo vetor de U, i.e:*

$$U^{\perp} = \{v \in V : v \cdot u = 0, \forall\ u \in U\}.$$

Observação 2.3. *O subconjunto $U^{\perp}$ é chamado* ***complemento ortogonal*** *de U e é também um subespaço vetorial de V.*

Definição 2.22. *Considere U e W subespaços vetoriais de V. A* ***soma*** *de U e W, denotada $U + W$ é definida por:*

$$U + W = \{u + w : u \in U \text{ e } w \in W\}$$

Observação 2.4. *A soma $U + W$ definida é subespaço vetorial de V.*

Definição 2.23. *O espaço vetorial V é a* ***soma direta*** *dos subespaços vetoriais U e W, denotado $V = U \oplus W$, se todo vetor $v \in V$ pode ser escrito de maneira única como $v = u + w$ tais que $u \in U$ e $w \in W$.*

Teorema 2.3. *Sejam U e W subespaços vetorias de V. Dizemos que $V = U \oplus W$ é soma direta de U e W, se e somente se:*

1. *$V = U + W$;*
2. *$U \cap W = \{0\}$.*

Observação 2.5. *Se V é soma direta de U e W, diz-se que U e W são subespaços vetorias complementares.*

Exemplo 2.9. *Sejam U e $U^{\perp}$ subespaços de $\mathbb{Z}_2^3$ assim definidos:*

$$U = \{(0,0,0), (1,0,1), (0,0,1), (1,0,0)\};$$

$$U^{\perp} = \{(0,0,0), (0,1,0)\};$$

Observe que $\mathbb{Z}_2^3 = U + U^{\perp}$ e $U \cap U^{\perp} = \{(0,0,0)\}$, com isso, conclui-se que $\mathbb{Z}_2^3 = U \oplus U^{\perp}$.

Definição 2.24. *Considere U e V espaços vetoriais sobre um corpo K. Dizemos que uma função $T : U \to V$ é uma* ***transformação linear*** *quando for satisfeita a seguinte condição:*

$$\forall u, v \in U, \quad \forall \lambda \in K, \quad T(u + \lambda v) = T(u) + \lambda T(v).$$

Seja $T : U \to V$ uma transformação linear. Define-se o ***núcleo de T*** *como sendo o subespaço vetorial de U definido por:*

$$ker\ T = \{u \in U : T(u) = 0\}.$$

E, define-se a ***imagem de T*** *como sendo o subespaço vetorial de V definido por:*

$$Im\ T = \{T(u) : u \in U\}.$$

2.2 Espaços Métricos

Definição 2.25. *Um conjunto não vazio M é dito um* ***espaço métrico*** *se existe uma função*

$$d : M \times M \to \mathbb{R},$$

chamada de ***métrica*** *ou* ***distância****, satisfazendo para todos $x, y, z \in M$ as seguintes propriedades:*

1. *$d(x, y) \geq 0$ e $d(x, y) = 0$ se e somente se, $x = y$;*
2. *$d(x, y) = d(y, x)$;*
3. *$d(x, z) = d(x, y) + d(y, z)$.*

Exemplo 2.10. *Um conjunto M é um espaço métrico associado a métrica definida por:*

$$d(x, y) = \begin{cases} 0, & \text{se } x = y \\ 1, & \text{se } x \neq y \end{cases}$$

e denominada ***métrica discreta****.*

Exemplo 2.11. *Sejam M^n um espaço n-dimensional e a métrica*

$$d_H = \sum_{i=1}^{n} d(x_i, y_i)$$

com $d(x_i, y_i)$, para cada $i \in \{1, 2, \cdots, n\}$, é a métrica discreta. Logo, d_H é uma métrica em M^n denominada ***métrica ou distância de Hamming****.*

2.3 Códigos de Bloco Lineares

Considere um corpo finito $K = \mathbb{F}_q$ com q elementos como sendo o alfabeto. Logo, para cada natural n temos um espaço vetorial sobre $K = \mathbb{F}_q$ de dimensão n denotado por $K^n = \mathbb{F}_q^n$.

Definição 2.26. *Um subconjunto não vazio $\mathcal{C} \subset \mathbb{F}_q^n$ é chamado um* ***código de bloco linear*** *se for um subespaço vetorial de $\mathbb{F}_q^n$. Chama-se* ***palavras-código*** *os elementos de $\mathcal{C}$.*

Definição 2.27. *Dado $u \in \mathbb{F}_q^n$, definimos o* ***peso*** *de u como sendo o número inteiro:*

$$\omega(u) = d(u, 0) = |\{i : u_i \neq 0, 1 \leq i \leq n\}|$$

onde 0 denota o vetor nulo. O peso de $\mathcal{C}$ é o inteiro:

$$\omega(\mathcal{C}) = \min\{\omega(u) : u \in \mathcal{C}\}.$$

A **distância mínima** de $\mathcal{C}$ é equivalente a:

$$d(\mathcal{C}) = \min\{\omega(x) : x \in \mathcal{C}, x \neq 0\},$$

dado que $d(u, v) = d(u - v, 0) = \omega(u - v)$ e $\mathcal{C}$ é um espaço linear.

Os **paramêtros** de um código de bloco linear $\mathcal{C}$ é definido por (n, k, d), onde n é o comprimento das palavras-código de $\mathcal{C}$, k é a dimensão de $\mathcal{C}$ sobre $\mathbb{F}_q$ e d é a distância mínima de $\mathcal{C}$. Note que o número de elementos de $\mathcal{C}$ é dado por $|\mathcal{C}| = |\mathbb{F}_q|^k = q^k$, onde a operação $|\cdot|$ representa a cardinalidade do conjunto.

Observação 2.6. *Uma forma de descrever subespaços vetoriais de um espaço vetorial $\mathbb{F}_q^n$ é como imagem de um transformação linear:*

$$\phi : \mathbb{F}_q^k \to \mathbb{F}_q^n$$
$$(a_1, a_2, \cdots, a_k) \to G_{n\times k}(a_1, a_2, \cdots, a_k)^\top,$$

onde $G_{n\times k}$ é uma matriz formada por elementos de $\mathbb{F}_q$.

Exemplo 2.12. *Uma **matriz geradora** de um código de bloco linear $\mathcal{C}$ com paramêtros (n, k, d) é uma matriz $G_{k\times n}$ cujas linhas formam uma base para $\mathcal{C}$.*

Observação 2.7. *Observe que a matriz geradora do código $\mathcal{C}$ é $G_{k\times n} = G_{n\times k}^\top$ e que pode não ser única dado que em um espaço(subespaço) vetorial pode existir mais de uma base.*

Definição 2.28. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código de bloco linear com parâmetros (n, k, d). Chamamos de **código dual** de $\mathcal{C}$, denotado por $\mathcal{C}^\perp$, o complemento ortogonal do subespaço vetorial $\mathcal{C}$ de $\mathbb{F}_q^n$,*

$$\mathcal{C}^\perp = \{v \in \mathbb{F}_q^n : v \cdot u = 0,\ \forall u \in \mathcal{C}\}.$$

*Uma matriz **verificação de paridade** H para um código de bloco linear $\mathcal{C}$ é uma matriz geradora para o código dual $\mathcal{C}^\perp$, cuja ordem é $(n - k) \times n$.*

Observação 2.8. *O código dual $\mathcal{C}^\perp$ é um subespaço vetorial de $\mathbb{F}_q^n$.*

Teorema 2.4. *(**Limitante de Singleton**) Um código de bloco linear $\mathcal{C} \subseteq \mathbb{F}_q^n$ com parâmetros (n, k, d) satisfaz:*

$$q^k \leq q^{n-d+1}$$

ou

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

dado que $q > 0$.

Exemplo 2.13. *O conjunto $\mathcal{C} = \{0000, 1011, 1101, 0110\} \subset \mathbb{Z}_2^4$ é um subespaço vetorial. Uma base para $\mathcal{C}$ é o conjunto $B = \{1011, 1101\}$. Temos que:*

$$\omega(1011) = 3, \qquad \omega(1101) = 3, \qquad \omega(0110) = 2,$$

logo a distância mínima de $\mathcal{C}$ é 2 e portanto trata-se de um código com paramêtros $(n, k, d) = (4, 2, 2)$. A matriz geradora de $\mathcal{C}$ é:

$$G_{k\times n} = G_{2\times 4} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

A matriz geradora também pode ser obtida por meio da transformação linear:

$$\phi : \mathbb{Z}_2^2 \to \mathbb{Z}_2^4$$
$$(a_1, a_2) \to (a_1 + a_2, a_2, a_1, a_1 + a_2)$$
$$(a_1, a_2) \to \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} .a_1 \\ a_2 \end{bmatrix}$$

Como, $G_{4\times 2} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$, *segue que a matriz geradora do código $\mathcal{C}$ é* $G_{2\times 4} = G_{4\times 2}^{\top} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$.

2.4 Conceitos de Design Combinatório

Nesta seção, apresentamos os conceitos de design combinatório, uma estrutura combinatória que por meio dos trabalhos de Euler sobre quadrados latinos no fim do século XVIII teve suas origens mais formais. Esta área possui fortes conexões com outras áreas da matemática, tais como: teoria de grupos, teoria de corpos finitos, teoria dos números e teoria de geometrias finitas, etc. É dessa diversidade que podemos encontrar diversos exemplos de aplicações em áreas, como Teoria da Informação, Estatística, Biologia e Engenharia (BRAUN *et al.*, 2013; BRAUN *et al.*, 2016; STINSON, 2004; COULBORN; DINITZ, 2007).

Definição 2.29. *Seja $X \neq \emptyset$ um conjunto com v elementos e $B \neq \emptyset$ uma coleção de b subconjuntos distintos de X com cardinalidade $k > 0$. Definimos o par (X, B) por* ***t-design*** *com parâmetros (v, k, λ), onde $0 < t < k < v$ e $\lambda > 0$, se cada subconjunto de cardinalidade t está contido em exatamente λ elementos de B. Usualmente os elementos de B são chamados* ***blocos****.*

Exemplo 2.14. *O par (X, B) com $X = \{0, 1, 2, 3, 4, 5, 6, 7\}$ e com o conjunto de blocos $B = \{0145, 2367, 0246, 1357, 0347, 1256, 0123, 4567, 0167, 2345, 0257, 1346, 0356, 1247\}$ é um 3-design com parâmetros $(8, 4, 1)$, ou seja, a cardinalidade de X é $v = 8$, cada bloco de B é formado por quatro elementos, isto é, $k = 4$ e cada subconjunto de três elementos de X está contido em apenas um bloco.*

Exemplo 2.15. *O par* (X, B) *com* $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ *e com o conjunto de blocos* $B = \{0123, 0145, 0246, 0378, 0579, 0689, 1278, 1369, 1479, 1568, 2359, 2489, 2567, 3458, 3467\}$ *é um 2-design com parâmetros* $(10, 4, 2)$*, isto é, a cardinalidade de* X *é* $v = 10$*, cada bloco de* B *é formado por quatro elementos, ou seja,* $k = 4$ *e cada subconjunto de dois elementos de* X *está contido em dois blocos.*

Neste trabalho, daremos atenção especial a uma classse de design do tipo $t = 2$. Para esta classe daremos a seguinte definição.

Definição 2.30. *Sejam* $X \neq \emptyset$ *um conjunto com* v *elementos e* $B \neq \emptyset$ *uma coleção de subconjuntos distintos de* X *com cardinalidade* b*. Definimos o par* (X, B) *por* ***t-design*** *com parâmetros* (v, k, λ)*, onde* $0 < k < v$ *e* $\lambda > 0$*, e escreve* (v, k, λ)***-design****, se:*

- *cada bloco de* B *contém exatamente* k *elementos;*
- *cada par de elementos distintos de* X *está contido em exatamente* λ *blocos.*

Observação 2.9. *Uma outra forma de denotar a classe dos design da Definição 2.30 é* (v, k, λ)***-BIBD*** *(do Inglês,* ***B****alanced* ***I****ncomplete* ***B****lock* ***D****esign).*

Exemplo 2.16. *Considere o conjunto* $X = \{1, 2, 3, 4, 5, 6, 7\}$ *com* $B = \{123, 145, 167, 247, 256, 346, 357\}$*. O par* (X, B) *é um* $(7, 3, 1)$*-BIBD.*

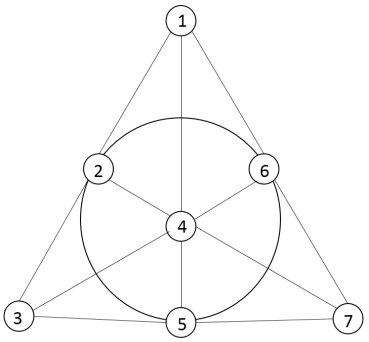


Figura 4 – Plano de Fano

A seguir, apresentamos algumas relações existentes entre os parâmetros de um (v, k, λ)-BIBD.

Proposição 2.1. *Se* (X, B) *é um* (v, k, λ)*-BIBD, então cada elemento de* X *pertence a* r *blocos, onde:*

$$bk = rv \quad e \quad r(k-1) = \lambda(v-1). \tag{2.1}$$

Observação 2.10. *Na literatura também encontra-se a seguinte notação par esta classe de design* (v, b, r, k, λ)***-BIBD*** *(STINSON, 2004; COULBORN; DINITZ, 2007).*

A Proposição 2.1, nos diz que não existem (v, k, λ)-BIBD com parâmetros que não satisfaçam as equações (2.1).

Exemplo 2.17. *Não existem (v, k, λ)-BIBD com os parâmetros $(8, 3, 1)$ ou $(11, 6, 2)$.*

Apresentamos, a seguir, um resultado mais geral, válido para qualquer t-design.

Proposição 2.2. *Se (X, B) é um t-design com parâmetros (v, k, λ), com $0 < t < k < v$ e $\lambda > 0$, então o número de blocos b é dado por:*

$$b\binom{k}{t} = \lambda\binom{v}{t}.$$

Definimos a seguir uma importante classe de design, onde a cardinalidade do conjunto X é igual a cardinalidade do conjunto dos blocos B.

Definição 2.31. *Um (v, k, λ)-BIBD (X, B) diz-se **simétrico** se $\mid X \mid = \mid B \mid = v = b$.*

Observação 2.11. *Das equações (2.1) e da Definição 2.31, pode-se concluir que se um (v, k, λ)-BIBD é simétrico, então $k = r$.*

Exemplo 2.18. *Sejam $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D\}$ e $B = \{1234, 1567, 189A, 1BCD, 258B, 269D, 27AC, 359C, 36AB, 378D, 45AD, 468C, 479B\}$. Assim, o par (X, B) é um $(13, 4, 1)$-BIBD simétrico, onde $b = v = 13$ e $r = k = 4$.*

Muitas vezes é conveniente representar o design por meio de uma matriz de incidência, definida a seguir.

Definição 2.32. *Seja (X, B) um design, onde $X = \{x_1, \cdots, x_v\}$ e $B = \{B_1, \cdots, B_b\}$. A **matriz de incidência** de (X, B) é uma matriz M, onde os elementos $m_{i,j}$ são definidos pela seguinte regra*

$$m_{i,j} = \begin{cases} 1, & \text{se } x_i \in B_i \\ 0, & \text{se } x_i \notin B_i \end{cases}. \tag{2.2}$$

A matriz de incidência M de um (v, k, λ)-BIBD satisfaz as seguintes propriedades:

- *cada coluna de M contém exatamente k "1"s.*
- *cada linha de M contém exatamente r "1"s.*
- *Duas linhas distintas de M ambas contém "1"s em exatamente λ colunas.*

Exemplo 2.19. *Sejam* $X = \{1, 2, 3, 4\}$ *e* $B = \{123, 234, 134, 124\}$. *O par* (X, B) *é um* $(4, 3, 2)$*-BIBD cuja matriz de incidência é:*

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

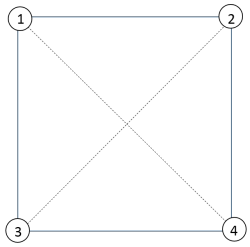


Figura 5 – Geometria do Design $(4, 3, 2)$-BIBD

Uma outra classe importante de design que aparece no decorrer do trabalho é a classe chamada design balanceado aos pares - PBD, (do Inglês, **P**airwise **B**alanced **D**esigns) .

Definição 2.33. *Um* ***design balanceado aos pares - PBD*** *é um design* (X, B) *tal que cada par de pontos distintos de* X *está contido em exatamente* λ *blocos, onde* λ *é um inteiro positivo. Além disso,* (X, B) *é um* ***design balanceado aos pares regular - PBD Regular*** *se todos os pontos* $x \in X$ *ocorrem exatamente em* r *blocos* $B_{i's} \in B$*, em que* r *é um inteiro positivo.*

Exemplo 2.20. *Sejam o design balanceado aos pares regular - PBD Regular com* $X = \{1, 2, 3, 4, 5, 6\}$ *e* $B = \{123, 456, 14, 15, 16, 24, 25, 26, 34, 35, 36\}$. *Assim, a cardinalidade de* X *é* $v = 6$*, a cardinalidade de* B *é* $b = 11$*,* $r = 4$*, ou seja, o número de blocos em que cada elemento de* X *está contido, e* $\lambda = 1$ *pelo fato de que a cada par de elementos de* X *está contido em apenas 1 bloco. Sua matriz de incidência é:*

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

Observação 2.12. *O design do Exemplo 2.20 não é BIBD, visto que temos blocos de tamanho k=3 e de tamanho k=2. No design balanceado aos pares - PBD o valor de k pode variar.*

2.4.1 Quadrados Latinos e Sistema de Steiner

Nesta seção, apresentamos a definição de quadrados latino e a definição de sistema de Steiner. Também, apresentamos duas construções importantes de designs, as construções de Bose e de Skolem. Sugerimos (STINSON, 2004; COULBORN; DINITZ, 2007) para maiores detalhes das construções e demonstrações dos resultados aqui apresentados.

Definição 2.34. *Um **quadrado latino** de ordem n com entradas em um conjunto X de n elementos é uma matriz S, $n \times n$, tal que cada elemento ocorre exatamente uma vez em cada linha e uma vez em cada coluna.*

Exemplo 2.21. *Um quadrado latino de ordem 3 é:*

$$S = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \tag{2.3}$$

Definimos, também, um objeto algébrico que está intimamente relacionado aos quadrados latinos, os chamados quasigrupos.

Definição 2.35. *Seja X um conjunto finito de cardinalidade n, e seja $\circ$ uma operação binária definida em X, isto é, $\circ : X \times X \to X$. Dizemos que o par $(X, \circ)$ é um **quasigrupo** de ordem n, se as duas propriedades seguintes são satisfeitas:*

- *Para cada $x, y \in X$, a equação $x \circ z = y$ tem uma única solução para $z \in X$.*
- *Para cada $x, y \in X$, a equação $z \circ x = y$ tem uma única solução para $z \in X$.*

Teorema 2.5. *Suponha que $\circ$ é uma operação binária definida em um conjunto X de cardinalidade n. Então, $(X, \circ)$ é um quasigrupo se, e somente se, com esta operação $A = (a_{x,y})$, onde $a_{x,y} = x \circ y$, é um quadrado latino de ordem n.*

Definição 2.36. *Suponha que $(X, \circ)$ é um quasigrupo. Dizemos que $(X, \circ)$ é **idempotente** se $x \circ x = x$ para todo $x \in X$, e dizemos que $(X, \circ)$ é um quasigrupo **simétrico** se $x \circ y = y \circ x$ para todo $x, y \in X$.*

Teorema 2.6. *Existe um quasigrupo idempotente simétrico de ordem n se, e somente se, n é ímpar.*

Definição 2.37. *Um t-design com parâmetros $(v, k, 1)$ é definido como sendo um **sistema de Steiner** e denota-se por $S(t, v, k)$.*

Um caso particular de sistema de Steiner são os sistema triplo de Steiner com $k = 3$.

Definição 2.38. *Definimos um* ***sistema triplo de Steiner*** *de ordem v e denotamos por $STS(v)$ como sendo um sistema de Steiner com parâmetros $S(2, v, 3)$*

Observação 2.13. *Um sistema triplo de Steiner $STS(v)$ é um $(v, 3, 1)$-BIBD ou um $(v, 3, 1)$-PBD.*

Uma condição necessária para a existência de um sistema triplo de Steiner é apresentada através da seguinte proposição.

Proposição 2.3. *Uma condição necessária para que exista um sistema triplo de Steiner de ordem v, com $v \geq 3$, é que $v \equiv 1$ mod 6 ou $v \equiv 3$ mod 6.*

Apresentamos, a seguir, duas técnicas para a construção de sistema triplo de Steiner.

A **construção de Bose** é uma técnica aplicada para construção de sistema triplo de Steiner de ordem $v \equiv 3$ *mod* 6, descrita da seguinte forma:

Seja um conjunto S (conjunto de pontos do sistema triplo de Steiner $STS(v)$) definido como sendo $S = Q \times \mathbb{Z}_3$, onde Q é um quasigrupo idempotente simétrico de ordem $2n + 1$, ou seja, ímpar e $\mathbb{Z}_3 = \{0, 1, 2\}$.

Para cada $q \in Q$, considere o seguinte conjunto:

$$A_q = \{(q, 0), (q, 1), (q, 2)\}.$$

Agora, para cada $q, r \in Q$, com $q < r$, e para cada $i \in \mathbb{Z}_3$, considere o conjunto:

$$B_{q,r,i} = \{(q, i), (r, i), (q \circ r, (i + 1) mod\ 3\}.$$

Disso, define-se β como sendo o conjunto dado por

$$\beta = \{A_q : q \in Q\} \cup \{B_{q,r,i} : q, r \in Q, q < r, i \in \mathbb{Z}_3\}.$$

Assim, o par (S, β) define um $STS(v)$ de ordem $v = 6n + 3 = 3(2n + 1)$.

Teorema 2.7. *Existe um $STS(v)$ para todo $v \equiv 3$ mod 6, onde $v \geq 9$.*

Exemplo 2.22. *Vamos construir o STS(9), ou seja, $v = 9$. Assim, $n = 1$, e portanto, devemos obter um quasigrupo idempotente simétrico de ordem 3. Logo, $Q = \{0, 1, 2\}$ e com isso $S = Q \times \mathbb{Z}_3 = \{0, 1, 2\} \times \{0, 1, 2\}$, o conjunto de pares ordenados. O quasigrupo idempotente simétrico de ordem 3 $(Q, \circ)$ é:*

$\circ$	**0**	**1**	**2**
0	0	2	1
1	2	1	0
2	1	0	2

Tabela 1 – Quasigrupo Idempotente Simétrico de Ordem 3

Agora, basta apresentar o conjunto β de triplas.

Primeiro caso: $A_q = \{(q,0),(q,1),(q,2)\}$,*tal que* $0 \leq q \leq 2$.

$$q = 0 : \{(0,0),(0,1),(0,2)\}$$
$$q = 1 : \{(1,0),(1,1),(1,2)\}$$
$$q = 2 : \{(2,0),(2,1),(2,2)\}$$

Segundo caso: $B_{q,r,i} = \{(q,i),(r,i),(q \circ r,(i+1)mod\ 3)\}$, *tal que* $0 \leq q < r \leq 2$ *e* $0 \leq i \leq 2$. *Assim,*

$$q = 0\ e\ r = 1 : \{(0,0),(1,0),(2,1)\},\{(0,1),(1,1),(2,2)\},\{(0,2),(1,2),(2,0)\}$$
$$q = 0\ e\ r = 2 : \{(0,0),(2,0),(1,1)\},\{(0,1),(2,1),(1,2)\},\{(0,2),(2,2),(1,0)\}$$
$$q = 1\ e\ r = 2 : \{(1,0),(2,0),(0,1)\},\{(1,1),(2,1),(0,2)\},\{(1,2),(2,2),(0,0)\}$$

Portanto, o par (S,β) *nessas condições, define um* $STS(9)$.

A **construção de Skolem** é uma outra técnica aplicada para a construção de sistema triplo de Steiner semelhante à construção de Bose, porém de ordem $v \equiv 1\ mod\ 6$. No caso da construção de Skolem usa-se o conceito de **quasigrupo semi-idempotente**, condicionado à:

$$q \circ q = \begin{cases} q, & se\ \ 0 \leq q < \frac{n}{2} \\ q - \frac{n}{2}, & se\ \ \frac{n}{2} \leq q < n \end{cases},$$

onde $q \in Q = \{0,\cdots,n-1\}$, quando n é par. Considere um conjunto S (conjunto de pontos do sistema triplo de Steiner STS(v)) como sendo $S = (Q \times \mathbb{Z}_3) \cup \{\infty\}$, onde Q é um quasigrupo semi-idempotente simétrico de ordem $2n$, $\mathbb{Z}_3 = \{0,1,2\}$ e ∞ é apenas um símbolo para representar a ordem 1 na expressão $v = 1 + 3(2n)$.

Para cada $q \in Q$, tal que $0 \leq q \leq n-1$, consideremos o seguinte conjunto:

$$A_q = \{(q,0),(q,1),(q,2)\}.$$

Assim, para cada $q,r \in Q$, $q < r$ e para cada $i \in \mathbb{Z}_3$, consideremos o conjunto:

$$B_{q,r,i} = \{(q,i),(r,i),(q \circ r,(i+1)mod\ 3)\}.$$

Finalmente, para $0 \leq q \leq n-1$ e para cada $i \in \mathbb{Z}_3$, consideremos o conjunto:

$$C_{q,i} = \{\infty,(q+n,i),(q,(i+1)mod\ 3)\}.$$

Portanto, definimos o conjunto de blocos:

$$\beta = \{A_q : 0 \leq q \leq n-1\} \cup \{B_{q,r,i} : q,r \in Q, q < r, i \in \mathbb{Z}_3\} \cup \{C_{q,i} : 0 \leq q \leq n-1, i \in \mathbb{Z}_3\}.$$

Com isso, o par (S,β) define um $STS(v)$ de ordem v.

Teorema 2.8. *Existe um quasigrupo semi-idempotente simétrico de ordem n se, e somente se, n é par.*

Teorema 2.9. *Existe um $STS(v)$ para todo $v \equiv 1 \ mod \ 6$, com $v \geq 7$.*

Exemplo 2.23. *$(Q, \circ)$ é um quasigrupo semi-idempotente de ordem 4 usado na construção do $STS(13)$ via construção de Skolem:*

$\circ$	**0**	**1**	**2**	**3**
0	0	2	1	3
1	2	1	3	0
2	1	3	0	2
3	3	0	2	1

Tabela 2 – Quasigrupo Idempotente Simétrico de Ordem 4

2.5 Conceitos de Conjuntos Parcialmente Ordenados

Nesta seção, apresentamos os conceitos de conjuntos parcialmente ordenados, que serão importantes, principalmente para o desenvolvimento do Capítulo 4.

Definição 2.39. *Seja P um conjunto não vazio. Dizemos que uma relação binária é um* ***ordem parcial*** *em P, normalmente denotada por "$\leq$", se possui as seguintes propriedades (ROMAN, 2008):*

- *$a \leq a$, para todo $a \in P$ (reflexiva);*
- *Se $a, b \in P$ são tais que $a \leq b$ e $b \leq a$, então $a = b$ (anti-simétrica);*
- *Se $a, b, c \in P$ são tais que $a \leq b$ e $b \leq c$, então $a \leq c$ (transitiva).*

Observação 2.14. *Neste contexto, dizemos que $(P, \leq)$ é um conjunto parcialmente ordenado. Podemos dizer ainda que se $a \leq b$ então a precede b, e que a e b são comparavéis. Dizemos ainda que b é um sucessor de a se $a < b$ e se não existe $x \in P$ tal que $a < x < b$.*

Definição 2.40. *Seja "$\leq$"uma ordem parcial em P. Se $a \leq b$ ou $b \leq a$, para quaisquer $a, b \in P$, dizemos que "$\leq$"é uma* ***ordem total*** *e que P é um* ***conjunto totalmente ordenado****.*

Definição 2.41. *Definimos o* ***comprimento (ou altura)*** *de um conjunto ordenado P, e denotamos por $l(P)$, como sendo:*

$$l(P) = max\{n \in \mathbb{N}; n \in \zeta\}$$

se P tem comprimento finito e ζ representa o conjunto de comprimentos finitos. Se $\{n \in \mathbb{N}; n \in \zeta\}$ é ilimitado definimos $l(P) = \infty$.

Exemplo 2.24. *Sendo G um grupo, o conjunto dos subgrupos de G, munido da relação de inclusão, é um conjunto parcialmente ordenado, normalmente denotado por $R(G)$.*

Exemplo 2.25. *O conjunto $\mathbb{N}$ dos números naturais, munido da relação de divisibilidade é um conjunto parcialmente ordenado.*

Observação 2.15. *O conjunto $\mathbb{Z}$ dos inteiros não pode ser ordenado pela relação de divisibilidade. De fato, dado $a \in \mathbb{Z}$ não nulo, temos que -a divide a e a divide -a, mas $-a \neq a$. Logo, a propriedade de anti-simétrica não é valida.*

Exemplo 2.26. *Sejam P_1 e P_2 conjuntos ordenados. Considerando o produto cartesiano $P_1 \times P_2$, vamos definir a relação*

$$(x_1, y_1) \leq (x_2, y_2) \quad se \quad x_1 \leq x_2 \quad e \quad y_1 \leq y_2.$$

Assim, $P_1 \times P_2$ munido desta relação é um conjunto parcialmente ordenado, chamado de produto direto de P_1 e P_2.

Definição 2.42. *Sejam P um conjunto parcialmente ordenado $\emptyset \neq S \subseteq P$ e $x \in S$. Dizemos que:*

- *x é um **elemento minimal** de S, se não existe $s \in S$ tal que $s < x$.*
- *x é um **elemento maximal** de S, se não existe $s \in S$ tal que $x < s$.*

Definição 2.43. *Sejam P um conjunto parcialmente ordenado $\emptyset \neq S \subseteq P$ e $x \in S$. Dizemos que:*

- *x é uma **cota inferior** de S, se $x \leq s$ para todo $s \in S$.*
- *x é um **cota superior** de S, se $s \leq x$ para todo $s \in S$.*

Exemplo 2.27. *Em $\mathbb{R}$ não existem elementos maximais ou minimais com respeito a ordem usual.*

Exemplo 2.28. *Em D_{36} (Divisores de 36), considere o subconjunto $S = \{2, 3, 6, 12, 18\}$. Temos que 2 e 3 são elementos minimais e 12 e 18 são elementos maximais em S, mas não existe em S nem cota superior nem cota inferior.*

Uma maneira adequada para identificar relações hierárquicas entre determinados elementos é a utilização de diagramas. **Diagrama de Hasse** é uma ferramenta matemática que representa graficamente qualquer conjunto finito parcialmente ordenado e assim evidência as relações hierárquicas existentes entre os elementos que são comparáveis. Cosiderando-se um conjunto parcialmente ordenado P com uma ordem parcial " $\leq$ ", seu diagrama é construido da seguinte forma:

- Os elementos do conjunto são representados por pequenos círculos (ponto);
- Se $a \leq b$, então o círculo que representa b fica a direita do circulo que representa a;
- Se b é sucessor de a, então o círculo que representa a é conectado ao círculo que representa b por um segmento de reta.

2.5.1 Isomorfismo entre Conjuntos Parcialmente Ordenados

Definição 2.44. *Sejam P e Q dois conjuntos parcialmente ordenados. Dizemos que uma aplicação $\varphi : P \to Q$ é:*

- ***isótona**, se para $a, b \in P$ tais que $a \leq b$ tivermos $\varphi(a) \leq \varphi(b)$.*
- ***antítona**, se para $a, b \in P$ tais que $a \leq b$ tivermos $\varphi(b) \leq \varphi(a)$.*

Definição 2.45. *Um **isomorfismo de conjuntos ordenados** é definido como sendo uma aplicação bijetiva isótona com aplicação inversa isótona. Se existe um isomorfismo $\varphi : P \to Q$ dizemos que P e Q são conjuntos isomorfos, e denotamos por $P \simeq Q$.*

Exemplo 2.29. *Nem toda aplicação isótona possui inversa. De fato, basta considerarmos a aplicação $\varphi : D_6 - \{1\} \to D_9$ definida por:*

$$\varphi(x) = \begin{cases} 1, se & x = 2 \\ 3, se & x = 3 \\ 9, se & x = 6 \end{cases} .$$

Assim, $1 \leq 3$ em D_9, mas sequer $\varphi^{-1}(1)$ e $\varphi^{-1}(3)$ são comparáveis em $D_6 - \{1\}$.

Observação 2.16. *Se $\varphi : P \to Q$ é um isomorfismo de conjuntos ordenados e $x, y \in P$ são elementos distintos, então:*

$$x < y \leftrightarrow \varphi(x) < \varphi(y).$$

Portanto, todas as relações hierárquicas entre elementos são preservadas por isomorfismo, portanto possuem o mesmo diagrama de Hasse. A recíproca é verdadeira, ou seja, conjuntos parcialmente ordenados que possuem mesmo diagrama de Hasse são isomorfos.

Observação 2.17. *Todo conjunto parcialmente ordenado é isomorfo a ele mesmo. Observe também que se $\varphi : P \to Q$ é um isomorfismo, então a aplicação inversa $\varphi^{-1} : Q \to P$ também é um isomorfismo. De fato: Se $y_1, y_2 \in Q$, então existem $x_1, x_2 \in P$ tais que $\varphi(x_1) = y_1$ e $\varphi(x_2) = y_2$. Logo, $y_1 \leq y_2 \leftrightarrow \varphi(x_1) \leq \varphi(x_2) \leftrightarrow \varphi^{-1}(y_1) = x_1 \leq x_2 = \varphi^{-1}(y_2)$.*

Observação 2.18. *Sejam P e Q conjuntos ordenados e $\varphi : P \to Q$ um isomorfismo. Se P tem mínimo 0_p, então Q também possui mínimo e $\varphi(0_p) = 0_q$. De fato, se $y \in Q$, então $y = \varphi(x)$, com $x \in P$. Sendo $0_p \leq x$, tem-se $\varphi(0_p) \leq \varphi(x) = y$. Por analogia:*

- *$\varphi(1_p) = 1_q$, onde 1_p é o máximo em P, se existir.*
- *Se $x \in P$ é maximal, então $\varphi(x)$ é maximal em Q.*
- *Se $x \in P$ é minimal, então $\varphi(x)$ é minimal em Q.*

Definição 2.46. *Um isomorfismo de um conjunto parcialmente ordenado sobre ele mesmo é dito* ***automorfismo****.*

Definição 2.47. *Um* ***isomorfismo dual*** *é definido como sendo uma aplicação bijetiva, antítona e com inversa antítona.*

Definição 2.48. *Um isomorfismo dual de um conjunto sobre ele mesmo é definido como sendo um* ***automorfismo dual*** *ou* ***autodualidade****.*

Definição 2.49. *Sejam P um conjunto parcialmente ordenado e $B \subseteq P$ um subconjunto limitado superiormente, ou seja, que possui cota superior em P. Um elemento $b \in P$ será chamado* ***supremo*** *do conjunto B, quando b é a "menor"das cotas superiores de B em P, isto é:*

1. *Para todo $x \in B$, tem-se $x \leq b$;*
2. *Se $c \in P$ é tal que $x \leq c$ para todo $x \in B$, então $b \leq c$.*

Definição 2.50. *Sejam P um conjunto parcialmente ordenado e $A \subseteq P$ um subconjunto limitado inferiormente, ou seja, que possui cota inferior em P. Um elemento $a \in P$ será chamado* ***ínfimo*** *do conjunto A, quando a é a "maior"das cotas inferiores de A em P, isto é:*

1. *Para todo $y \in A$, tem-se $a \leq y$;*
2. *Se $c \in P$ é tal que $c \leq y$ para todo $y \in a$, então $b \leq c$.*

Observação 2.19. *Tanto o supremo quanto o ínfimo, quando existem, são únicos e são denotados, respectivamente, supB e infA.*

Definição 2.51. *Um conjunto parcialmente ordenado será dito um* ***reticulado*** *se nele existirem o supremo e o ínfimo de qualquer par de seus elementos.*

Exemplo 2.30. *Para todo grupo G, temos que $R(G)$ é um reticulado. De fato, dados dois subgrupos $H, N \leq G$, lembre que $H \cap N$ é o maior subgrupo contido em ambos. Além disso, claramente $H \subseteq \langle H \cup N \rangle$ e $N \subseteq \langle H \cup N \rangle$. Tomando, agora, K subgrupo de G tal que $H \subseteq K$ e $N \subseteq K$, segue que $H \cup N \subseteq K$, e assim $\langle H \cup N \rangle \subseteq K$.*

Exemplo 2.31. *O conjunto de todos os subespaços de um espaço vetorial, parcialmente ordenado pela inclusão, é um reticulado. Observe que o ínfimo de dois subespaços W_1 e W_2 é a sua interseção. Veja também que se W_3 é um subespaço tal que $W_1, W_2 \subseteq W_3$, então $W_1 + W_2 \subseteq W_3$, onde:*

$$W_1 + W_2 = \{w_1 + w_2; w_i \in W_i\}.$$

Assim, $W_1 + W_2$ é o supremo, ou seja, o menor subespaço que contém ambos.

Exemplo 2.32. *Sejam $G = \{e, a, b, c\}$ e " $*$ " uma operação em G definida segundo a tabela:*

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Tabela 3 – Grupo de Klein

Temos que G munido desta operação é um grupo, chamado de ***grupo de Klein****. Sabemos que seus subgrupos são exatamente $\{e\}, G, \langle a\rangle = \{e, a\}, \langle b\rangle = \{e, b\}, \langle c\rangle = \{e, c\}$. Logo, $R(G)$ possui exatamente 5 elementos, dos quais G e $\{e\}$ são, respectivamente, o máximo e o mínimo, os demais são incomparáveis dois a dois. Portanto, o reticulado do grupo de Klein, denotado por $R(G)$ é:*

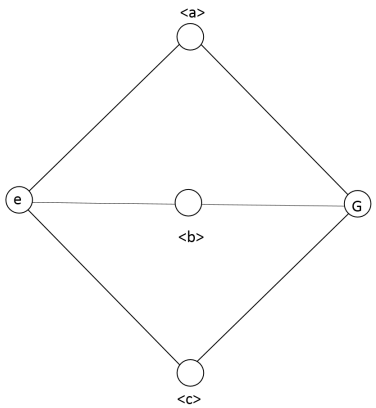


Figura 6 – Reticulado de Klein

Apresentamos nas Seções 2.6 e 2.7, dois conceitos fundamentais e importantes para o entendimento e desenvolvimento dos demais capítulos. O conceito de códigos geometricamente uniformes introduzido por (FORNEY, 1991), generalizou os códigos de Slepian (SLEPIAN, 1968) e os códigos reticulados, permitindo que os elementos do grupo sejam isometrias arbitrárias. E o conceito de códigos de subespaço introduzido por (KöETTER; KSCHISCHANG, 2008), mostram-se eficentes em controle de erros em codificação de rede.

2.6 Códigos Geometricamente Uniformes

Nesta seção, serão apresentadas algumas definições e resultados sobre códigos geometricamente uniformes, para maiores detalhes referimos o leitor para (FORNEY, 1991; SLEPIAN, 1968).

Definição 2.52. *Seja M um espaço métrico com uma métrica d e seja T uma transformação em M. Dizemos que T é uma* ***isometria*** *se T preserva a distância d, ou seja, $\forall$ $x,y \in M$ segue que $d(x,y) = d(T(x),T(y))$.*

Definição 2.53. *Uma* ***figura geométrica*** *S é um conjunto de pontos no $\mathbb{R}^n$. Duas figuras S_1 e S_2 são* ***geometricamente congruentes*** *se existe uma isometria u de $\mathbb{R}^n$ tal que $u(S_1) = S_2$.*

Definição 2.54. *Duas figuras S_1 e S_2 são* ***geometricamente equivalentes*** *se existem uma isometria u e um escalar $\alpha > 0$ tal que $u(\alpha S_1) = S_2$.*

Definição 2.55. *Uma isometria u de $\mathbb{R}^n$ S-invariante (ou seja, $U(S) = S$) é denominada uma* ***simetria*** *de S.*

Observação 2.20. *As simetrias de S formam um grupo sob a composição de funções, chamado* ***grupo de simetrias*** *$\Gamma(S)$ de S.*

Definição 2.56. *Um* ***conjunto de sinais*** *S é um subconjunto discreto de um espaço métrico M. Um conjunto finito de sinais é chamado* ***constelação de sinais****.*

Definição 2.57. *Um conjunto de sinais S é* ***geometricamente uniforme*** *se dado dois pontos quaisquer s, $s' \in S$ existe uma isometria u tal que:*

- $u(s) = s'$
- $u(S) = S$.

Observação 2.21. *Chamamos* ***constelação uniforme*** *a um conjunto finito de sinais S geometricamente uniforme. Caso o conjunto de sinais S seja infinito, chamamos* ***arranjo regular***

Exemplo 2.33. *Uma constelação de sinais binária unidimensional $S = \{-1, 1\}$ é geometricamente uniforme. Basta observarmos que o grupo de simetrias $\Gamma(S) = V = \{e, v\}$, onde e indica a identidade e v indica uma reflexão em torno da origem, satisfaz*

$$v(1) = -1, \quad v(-1) = 1 \quad e \quad v(S) = S.$$

Exemplo 2.34. *Considere o conjunto* $S = \{(-1,1),(-1,-1),(1,-1),(1,1)\}$ *que formam um quadrado. Existem 8 simetrias deste quadrado, e estas simetrias são os elementos do grupo diedral* $D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$*, onde* r *denota a rotação de* $\frac{2\pi}{4}$ *e* s *denota a reflexão em torno de um eixo de simetria, o qual pode ser representado pelo seguinte grupo de matrizes ortogonais, dadas por*

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}.$$

Observação 2.22. *As quatros primeiras matrizes são os elementos de um subgrupo especial do grupo diedral* D_4 *que é o grupo das rotações* $R_4 = \{e, r, r^2, r^3\}$*. E as quatros últimas também é um subgrupo especial de* D_4 *que é o grupo das reflexões* $V^2 = \{s, rs, r^2s, r^3s\}$*. Nesse caso,* R_4 *é isomorfo a* $\mathbb{Z}_4$*, e* V^2 *é isomorfo a* $\mathbb{Z}_2^2$*.*

Definição 2.58. *Um* ***grupo gerador*** $U(S)$ *de* S *é o menor subgrupo de* $\Gamma(S)$ *suficiente para gerar* S*.*

Observação 2.23. *O conjunto de sinais* $S = \{-1, 1\}$ *é um caso de conjunto de sinais geometricamente uniforme que possui um único grupo gerador que é isomorfo a* $\mathbb{Z}_2$*.*

Observação 2.24. R_4 *e* V^2 *são subgrupos de* D_4 *que geram todos os vértices do quadrado iniciando de qualquer um dos vértices.*

Teorema 2.10. *O produto cartesiano de conjunto de sinais geometricamente uniforme é um conjunto de sinais geometricamente uniforme.*

Observação 2.25. *Uma observação interessante é que, se considerarmos a composição de isometrias para cada entrada separadamente, temos que o conjunto* $S = \{-1, 1, \cdots, -1, 1\}$ *ainda será uma constelação de sinais, cujo grupo gerador é* V^n *com* 2^n *elementos e é isomorfo a* $\mathbb{Z}_2^n$*.*

Apresentamos, a seguir, algumas definições que caracterizam propriedades simétricas importantes dos conjuntos de sinais geometricamente uniforme.

Definição 2.59. *Seja* $s \in S$*. O conjunto de todos os pontos de* $\mathbb{R}^n$ *que estão mais próximos de* s *que qualquer outro ponto* $s' \in S$ *é chamado* ***Região de Voronoi*** *associada a* s*. Tal conjunto será denotado por:*

$$R_V(s) = \{x \in \mathbb{R}^n : d(x,s) = \| x - s \|^2 = min_{s' \in S} d(x,s') = \| x - s' \|^2\}$$

Definição 2.60. *Seja* $s \in S$*. O conjunto dado por*

$$DP(s) = \{d(x,s') = \| s - s' \|^2; s' \in S\}$$

é chamado ***perfil de distância global****.*

Teorema 2.11. *(**Uniformidade Geométrica**) Se S é um conjunto de sinais geometricamente uniforme, então:*

a) Todas as regiões de Voronoi $R_V(s)$ são congruentes, ou seja, $R_V(s') = u[R_V(s)]$, onde u é uma isometria que leva s em s'.

b) O perfil de distância global $DP(s)$ é o mesmo para todo $s \in S$.

Exemplo 2.35. *Considere o conjunto de sinais $S = \{-1, 1\}$. A região de Voronoi associada ao ponto $1 \in S$ sendo $m = 0$ o ponto médio do segmento$[-1, 1]$ é dada por $R_V(1) = [0, \infty)$.*

Definição 2.61. *Uma **partição geometricamente uniforme** denotada por S/S' é uma partição do conjunto geometricamente uniforme S com grupo gerador $U(S)$ induzida por um subgrupo normal U' de $U(S)$. Os elementos da partição S/S' são os subconjuntos de S que correspondem às classes laterais de U' em $U(S)$.*

Teorema 2.12. *(**Partição Geometricamente Uniforme**) Se S/S' é uma partição geometricamente uniforme, então os subconjuntos de S nesta partição são geometricamente uniformes, mutuamente congruentes e tem U' como um grupo gerador comum.*

Os Teoremas 2.11 e 2.12 estão demonstrados em (FORNEY, 1991).

Exemplo 2.36. *Um código binário linear (n, k) é um subgrupo de $\mathbb{Z}_2^n$ de ordem k. Pelo Teorema 2.12 este subgrupo induz uma partição geometricamente uniforme do hipercubo em 2^{n-k} partições geometricamente uniformes e congruentes entre si. O código binário linear $(n, k) = (3, 1)$ é um subgrupo de $\mathbb{Z}_2^3$ de ordem 1. Logo, o cubo é particionado em 4 partições geometricamente uniformes e congruentes entre si.*

2.7 Espaços Projetivos e Códigos de Subespaços

Considerando que todo espaço vetorial de dimensão m sobre um corpo finito $\mathbb{F}_q$ é isomorfo a $\mathbb{F}_q^m$ apresentamos a seguir algumas definições importantes, que podem ser encontradas em (FORNEY, 1991; SLEPIAN, 1968).

Definição 2.62. *O **espaço projetivo** é definido como o conjunto de todos os subespaços vetoriais de $\mathbb{F}_q^m$ e é denotado por $\mathbb{P}(\mathbb{F}_q^m)$. Além disso, o conjunto de todos os subespaços com uma dada dimensão k é denominado **grassmanniana** e denotado por $\mathcal{G}(\mathbb{F}_q^m, k)$.*

Observação 2.26. *Note que:*

$$\mathbb{P}(\mathbb{F}_q^m) = \bigcup_{k=0}^{m} \mathcal{G}(\mathbb{F}_q^m, k).$$

Podemos combinar elementos do espaço projetivo de modo a obter outros elementos desse mesmo espaço. Apresentamos a seguir as definições de soma e interseção de subespaços.

Definição 2.63. *A **soma de subespaços** $V_1 + V_2$ é definida como o espaço gerado pelo conjunto $V_1 \cup V_2$, isto é,*

$$V_1 + V_2 = \{v_1 + v_2 : v_1 \in V_1, v_2 \in V_2\}, \tag{2.4}$$

é um subespaço vetorial de $\mathbb{P}(\mathbb{F}_q^m)$

Observe que a soma $V_1 + V_2$ é o menor subespaço de $\mathbb{P}(\mathbb{F}_q^m)$ que contém simultaneamente V_1 e V_2.

Definição 2.64. *A **interseção de subespaços** $V_1 \cap V_2$ é definida como no sentido usual da teoria dos conjuntos, isto é,*

$$V_1 \cap V_2 = \{v : v \in V_1, v \in V_2\}, \tag{2.5}$$

é um subespaço vetorial de $\mathbb{P}(\mathbb{F}_q^m)$.

Observe que a interseção $V_1 \cap V_2$ é o maior subespaço de $\mathbb{P}(\mathbb{F}_q^m)$ que está contido simultualmente em V_1 e V_2.

Observação 2.27. *As dimensões do subespaço interseção e do subespaço soma se relacionam através de:*

$$dim(V_1 + V_2) = dimV_1 + dimV_2 - dim(V_1 \cap V_2). \tag{2.6}$$

Definição 2.65. *O **número de subespaços vetoriais** de $\mathbb{P}(\mathbb{F}_q^m)$ com dimensão k é dado por*

$$\binom{m}{k}_q = \prod_{i=0}^{k-1} \frac{q^m - q^i}{q^k - q^i}.$$

Definição 2.66. *A **cardinalidade de uma grassmanniana** de $\mathbb{P}(\mathbb{F}_q^m)$ com dimensão k é*

$$\mid \mathcal{G}(\mathbb{F}_q^m, k) \mid = \binom{m}{k}_q,$$

*e a **cardinalidade do espaço projetivo** de $\mathbb{P}(\mathbb{F}_q^m)$ é*

$$\mid \mathbb{P}(\mathbb{F}_q^m) \mid = \sum_{k=0}^{m} \binom{m}{k}_q.$$

Para a construção de códigos de subespaços é necessário associar ao espaço projetivo uma métrica ou distância, visto que códigos corretores ou detectores de erros nada

mais são que um espaço métrico discreto. A métrica ou distância associada que usamos é a distância de subespaço, responsável pela medida de correção e detecção de erros do código, permitindo uma forma de classificar e otimizar os códigos. Cabe lembrar que existem outras distâncias associadas ao espaço projetivo que o tornam também um espaço métrico, por exemplo, distância do posto, distância de injeção, entre outras (KHALEGHI *et al.*, 2009).

Definição 2.67. *Um* ***código de subespaço*** *é um conjunto não vazio de* $\mathbb{P}(\mathbb{F}_q^m)$*. No caso em que o código de subespaço está contido em uma grassmanniana de ordem k,* $\mathcal{G}(\mathbb{F}_q^m, k) = \{V \in \mathbb{P}(\mathbb{F}_q^m) : dimV = k\}$*, ou seja, todas as suas palavras códigos possuem a mesma dimensão,o código é chamado* ***código de subespaço de dimensão constante****. Denotamos por d a distância mínima do código* $\mathcal{C}$*.*

Definição 2.68. *A* ***distância de subespaço*** *entre* U *e* V *é definida como:*

$$d(U, V) = dim(U) + dim(V) - 2dim(U \cap V), \tag{2.7}$$

onde $\cap$ *representa a interseção (veja(2.5)) de subespaços.*

Teorema 2.13. $(\mathbb{P}(\mathbb{F}_q^m), d)$ *é um espaço métrico.*

Definição 2.69. *A* ***cardinalidade*** *do código* $\mathcal{C}$ *é dada por* $| \mathcal{C} | = M$ *e a* ***taxa do código*** *é definida por* $R(\mathcal{C}) = \frac{log|\mathcal{C}|}{m}$ *ou* $R(\mathcal{C}) = \frac{logM}{m}$ *medida em unidades de informação por uso de canal de subespaço, onde q é a base do logaritmo.*

Definição 2.70. *A* ***distância mínima*** *do código* $\mathcal{C}$ *é definida como:*

$$d = d(\mathcal{C}) = min\{d(U, V),\ U,\ V \in \mathcal{C},\ U \neq V\}.$$

Definição 2.71. *Seja* (m, M, d) *os* ***parâmetros*** *de um código* $\mathcal{C} \subset \mathbb{P}(\mathbb{F}_q^m)$*, onde m é a dimensão do espaço projetivo, M é a cardinalidade do código e d a distância mínima do código. Se o código* $\mathcal{C}$ *está em uma grassmanniana de dimensão k, então os parâmetros são* (m, M, d, k)*.*

Exemplo 2.37. *Considere o espaço vetorial* $\mathbb{F}_2^3$*. Um exemplo de código de subespaço no espaço projetivo* $\mathbb{P}(\mathbb{F}_2^3)$ *é considerar o código* $\mathcal{C}_1$ *como sendo o conjunto consistindo de três subespaços, isto é,* $\mathcal{C}_1 = \{S_1, S_2, S_3\}$*, onde* $S_1 = \{000, 100, 010, 110\}$*,* $S_2 = \{000, 001\}$*,* $S_3 = \{000, 111\}$*. Observe que* S_1 *tem dimensão 2 e* S_2, S_3 *tem dimensão 1. Observar também que não há interserções não nulas entre os subespaços* S_1, S_2 *e* S_3*. Assim, a distância entre* S_1 *e* S_2 *é dada por:*

$$d(S_1, S_2) = dim(S_1) + dim(S_2) - 2.dim(S_1 \cap S_2) = 2 + 1 - 0 = 3.$$

A distância entre S_1 *e* S_3 *é dada por:*

$$d(S_1, S_3) = dim(S_1) + dim(S_3) - 2.dim(S_1 \cap S_3) = 2 + 1 - 0 = 3.$$

A distância entre S_2 e S_3 é dada por:

$$d(S_2, S_3) = dim(S_2) + dim(S_3) - 2.dim(S_2 \cap S_3) = 1 + 1 - 0 = 2.$$

Portanto, $\mathcal{C}_1$ é um código com parâmetros $(m, M, d) = (3, 3, 2)$.

Exemplo 2.38. *Seja o espaço vetorial $\mathbb{F}_2^3$. Um exemplo interessante de código na grassmanniana é o código simplex $\mathcal{C}_2 = \{S_1, S_2, S_3\}$ com parâmetros $(n, M, d, k) = (3, 3, 2, 2)$, cujas palavras-código, ou seja, os subespaços vetoriais são $S_1 = \{000, 011, 100, 111\}$, $S_2 = \{000, 010, 101, 111\}, S_3 = \{000, 001, 110, 111\}$. Observe que os subespaços S_1, S_2, S_3 tem dimensão 2 e a intersecção entre quaisquer dois subespaços é o subespaço $\{000, 111\}$. Assim, a distância é dada por:*

$$d(S_i, S_j) = dim(S_i) + dim(S_j) - 2.dim(S_i \cap S_j) = 2 + 2 - 2.1 = 4 - 2 = 2,$$

para quaisquer $i, j \in \{1, 2, 3\}$ com $i \neq j$.

Uma forma de interpretar a distância de subespaço é por meio do diagrama de Hasse.

Diagrama de Hasse é uma ferramenta matemática que representa graficamente qualquer conjunto finito parcialmente ordenado. No nosso contexto, é possível construir o diagrama de Hasse, visto que o espaço projetivo $\mathbb{P}(F_q^m)$ com a seguinte relação de ordem $\preceq$, em que $S_1 \preceq S_2$ se, e somente se, S_1 é um subespaço de S_2, é parcialmente ordenado. Dois subespaços estão conectados, se e somente se, S_1 é um subespaço de S_2 e $dimS_2 = dimS_1 + 1$ ou vice-versa. Logo, a partir do diagrama de Hasse, podemos interpretar a distância entre dois subespaços S_1, S_2 de $\mathbb{P}(F_q^m)$ como o caminho de menor distância ligando S_1 e S_2 (geodésica).

Exemplo 2.39. *A Figura 7 ilustra o diagrama de Hasse do espaço projetivo $\mathbb{P}(\mathbb{F}_2^3)$.*

Observação 2.28.

1. *Usamos a notação S_i, onde $i \in \{1, 2, \cdots, 7\}$, para subespaços de dimensão 1 e S^j, onde $j \in \{1, 2, \cdots, 7\}$ para os subespaços de dimensão 2, que neste caso, são subespaços duais dos respectivos subespaços de dimensão 1.*

2. *O número de subespaços de dimensões 1 e 2 são iguais a 7. De fato,*

$$\binom{3}{2}_2 = \binom{3}{1}_2 = \frac{2^3 - 2^0}{2^1 - 2^0} = 7.$$

3. *Observe que as conexões da Figura 7 explicitam os subepaços de dimensão 1 que são subespaços dos subespaços de dimensão 2. Por exemplo, S_1 é um subespaço de S^2, S^4 e S^6.*

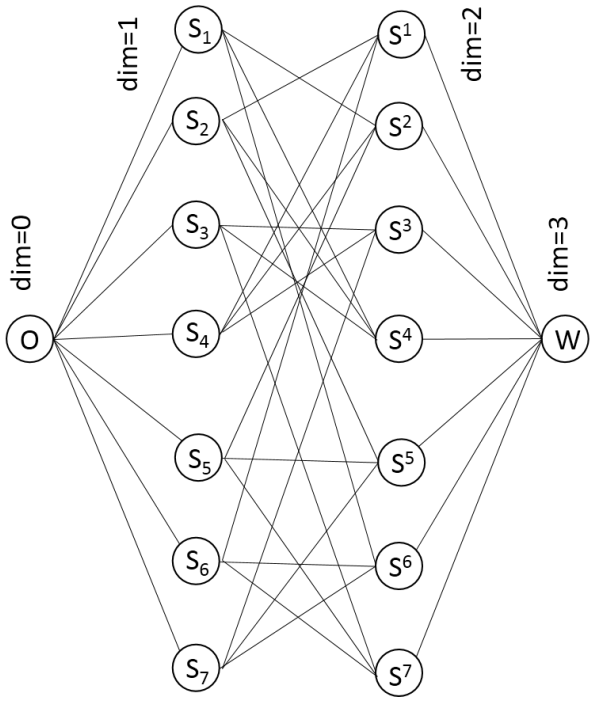


Figura 7 – Diagrama de Hasse do Espaço Projetivo de $\mathbb{F}_2^3$

Lema 2.1. *Sejam U e V subespaços de um espaço vetorial de dimensão n. Então, a distância é máxima, isto é, $d(U,V) = n$, se, e somente se,*

1. Os subespaços U e V se intersectam em um subespaço de dimensão 0,

2. $dim(U) + dim(V) = n$.

Exemplo 2.40. *Considere os subespaços S_1, S_2, S_3, S_4 como elementos da grassmanniana $\mathcal{G}(F_2^4, 2)$ dados por:*

$$S_1 = \{0000, 1000, 0100, 1100\} \qquad S_2 = \{0000, 0010, 0001, 0011\}$$

$$S_3 = \{0000, 1000, 0010, 1010\} \qquad S_4 = \{0000, 0100, 0010, 0110\}.$$

A distância de subespaço entre S_1 e S_2 é dada por:

$$d_s(S_1, S_2) = dimS_1 + dimS_2 - 2dim(S_1 \cap S_2) = 2 + 2 - 0 = 4.$$

Já a distância de subespaço entre S_1 e S_3 é dada por:

$$d_s(S_1, S_3) = dimS_1 + dimS_3 - 2dim(S_1 \cap S_3) = 2 + 2 - 2.1 = 2.$$

Observação 2.29. *Observe que entre os subespaços S_1 e S_2 a distância de subespaço é máxima. Quando ocorre da distância de subespaço ser máxima, podemos interpretar no Exemplo 2.40 que $S_1 \oplus S_2 = \mathbb{F}_2^4$, ou seja, $\mathbb{F}_2^4 = S_1 + S_2$ e $S_1 \cap S_2 = \{0\}$. Cabe observar*

que vale a propriedade de que todo elemento $u \in \mathbb{F}_2^4$ se decompõe de maneira única como soma de dois elementos v e w, sendo $u \in S_1$ e $w \in S_2$, isto é, $u = v + w$. O mesmo não ocorre entre S_1 e S_3.

3 Códigos de Subespaços *n*-shot Geometricamente Uniforme

Apresentamos nas Seções 2.6 e 2.7, dois conceitos importantes para o desenvolvimento deste capítulo, o conceito de códigos geometricamente uniformes e o conceito de códigos de subespaço, respectivamente. Em (NóBREGA; UCHôA-FILHO, 2009) é apresentada uma alternativa para obter códigos de subespaços com boas taxas e boas capacidades de correções de erros, sem a necessidade de aumentar a cardinalidade do corpo finito $\mathbb{F}_q$, ou do comprimento do vetor m, uma vez que, mesmo que seja possível ajustar os valores de q e m, questões de complexidade podem serem determinantes, por exemplo, a construção de códigos 1-shot em $\mathbb{P}(\mathbb{F}_q^{mn})$ são mais complexos que a construção de códigos n-shot em $\mathbb{P}(\mathbb{F}_q^m)^n$, logo, uma possibilidade é utilizar o canal n vezes, ou seja, codificar a informação em uma sequência de subespaços a ser enviada e não apenas em um único subespaço. Em (SILVA *et al.*, 2010) é apresentada a capacidade do canal matricial multiplicativo que é dada por:

$$C = log_q \sum_{k=0}^{n} \binom{m}{k}_q ,$$

q-ário em unidades por uso do canal. Tal resultado justifica a viabilidade de comunicação via subespaços, onde a informação é enviada na escolha do subespaço gerado pelas linhas da matriz de entrada.

Este capítulo está organizado da seguinte maneira. Na Seção 3.1, serão apresentadas as definições de extensão dos espaços projetivos, bem como os códigos de subespaços nessa extensão, chamados códigos de subespaços n-shot (NóBREGA; UCHôA-FILHO, 2009). Com isso em mente, e observado que códigos geometricamente uniformes são códigos com propriedades algébricas e geométricas interessantes tanto do ponto de vista matemático quanto de comunicações, além de possuírem eficientes algoritmos associados ao processo de decodificação. Na Seção 3.2, definimos o conceito de códigos de subespaços n-shot geometricamente uniforme e apresentamos alguns exemplos que descrevem uma nova classe de códigos com tais propriedades (LIMA; PALAZZO, 2017a; ROTMAN, 1993).

3.1 Espaços Projetivos Estendidos e Códigos de Subespaços *n*-shot

Com o objetivo de utilizar o canal de subespaço não apenas uma vez, onde se codifica a informação a ser transmitida em um único subespaço, mas utilizar n-vezes o canal, codificando a informação a ser transmitida em uma sequência de subespaços.

Apresentamos a seguir as principais definições e conceitos de espaços projetivos estendidos e códigos de subespaços n-shot.

Definição 3.1. *A **n-ésima extensão** do espaço projetivo $\mathbb{P}(\mathbb{F}_q^m)$ denotada por $\mathbb{P}(\mathbb{F}_q^m)^n$, é o n-ésimo produto cartesiano do espaço projetivo. Dessa forma, elementos de $\mathbb{P}(\mathbb{F}_q^m)^n$ são n-uplas tendo como componentes subespaços do espaço projetivo original $\mathbb{P}(\mathbb{F}_q^m)$.*

Definição 3.2. *A **distância (de subespaço estendida)** entre dois elementos $\boldsymbol{U} = (U_1, U_2, \cdots, U_n)$ e $\boldsymbol{V} = (V_1, V_2, \cdots, V_n)$ do espaço projetivo estendido $\mathbb{P}(\mathbb{F}_q^m)^n$ é definida como:*

$$d(\boldsymbol{U}, \boldsymbol{V}) = \sum_{i=1}^{n} d(U_i, V_i), \tag{3.1}$$

onde $d(U_i, V_i) = dim(U_i) + dim(V_i) - 2dim(U_i \cap V_i)$, para $i \in \{1, 2, \cdots, n\}$. Neste caso, $1 \leq d(\boldsymbol{U}, \boldsymbol{V}) \leq m.n$.

Teorema 3.1. *$(\mathbb{P}(\mathbb{F}_q^m)^n, d)$ é um espaço métrico.*

Demonstração: Sejam as seguintes n-tuplas de subespaços:

$$\boldsymbol{U} = (U_1, U_2, \cdots, U_n), \boldsymbol{V} = (V_1, V_2, \cdots, V_n), \boldsymbol{W} = (W_1, W_2, \cdots, W_n) \in \mathbb{P}(\mathbb{F}_q^m)^n.$$

Assim,

1) $d(\boldsymbol{U}, \boldsymbol{U}) = 0, \ \forall \ \boldsymbol{U} \in \mathbb{P}(\mathbb{F}_q^m)^n$, pois:

$$\begin{aligned} d(\boldsymbol{U}, \boldsymbol{U}) &= \textstyle\sum_{i=1}^{n} d(U_i, V_i) \\ &= \textstyle\sum_{i=1}^{n} (dim(U_i) + dim(U_i) - 2.dim(U_i \cap U_i) \\ &= \textstyle\sum_{i=1}^{n} (2.dim(U_i) - 2.dim(U_i) = 0. \end{aligned}$$

2) $d(\boldsymbol{U}, \boldsymbol{V}) > 0$ se $\boldsymbol{U} \neq \boldsymbol{V}$ e não são nulos simultaneamente, para $\boldsymbol{U}, \boldsymbol{V} \in \mathbb{P}(\mathbb{F}_q^m)^n$. Suponha, sem perda de generalidade, que, $\boldsymbol{U} \neq 0$ e $\boldsymbol{V} = 0$. Logo, $dim(\boldsymbol{U}) > 0$ e $dim(\boldsymbol{V}) = 0$. Como $dim(\boldsymbol{U} \cap \boldsymbol{V}) = 0$, segue que

$$\begin{aligned} d(\boldsymbol{U}, \boldsymbol{V}) &= \textstyle\sum_{i=1}^{n} d(U_i, V_i) \\ &= \textstyle\sum_{i=1}^{n} (dim(U_i) + dim(V_i) - 2.dim(U_i \cap V_i)) \\ &= \textstyle\sum_{i=1}^{n} dim(U_i) > 0. \end{aligned}$$

O mesmo acontecendo para $\boldsymbol{U} = 0$ e $\boldsymbol{V} \neq 0$. Agora, se $\boldsymbol{U} \neq \boldsymbol{V} \neq 0$, então $dim(\boldsymbol{U}) > 0$ e $dim(\boldsymbol{V}) > 0$. Como $dim(\boldsymbol{U} \cap \boldsymbol{V})$ é no máximo $dim(\boldsymbol{U}) > 0$ ou $dim(\boldsymbol{V}) > 0$, segue que $dim(\boldsymbol{U} \cap \boldsymbol{V}) \geq 0$. Assim,

$$\begin{aligned} d(\boldsymbol{U}, \boldsymbol{V}) &= \textstyle\sum_{i=1}^{n} d(U_i, V_i) \\ &= \textstyle\sum_{i=1}^{n} (dim(U_i) + dim(V_i) - 2.dim(U_i \cap V_i)) \\ &= \textstyle\sum_{i=1}^{n} (dim(U_i + V_i) + dim(U_i \cap V_i) - 2.dim(U_i \cap V_i)) \\ &= \textstyle\sum_{i=1}^{n} (dim(U_i + V_i) - dim(U_i \cap V_i) > 0. \end{aligned}$$

Observe que $dim(U_i + V_i) > dim(U_i \cap V_i)$.

3) $d(\boldsymbol{U}, \boldsymbol{V}) = d(\boldsymbol{V}, \boldsymbol{U})$. Isto é consequência direta da comutatividade das operações de soma e intersecção de subespaços. Assim,

$$\begin{aligned} d(\boldsymbol{U}, \boldsymbol{V}) &= \sum_{i=1}^{n} d(U_i, V_i) \\ &= \sum_{i=1}^{n} (dim(U_i) + dim(V_i) - 2.dim(U_i \cap V_i) \\ &= \sum_{i=1}^{n} (dim(V_i) + dim(U_i) - 2.dim(V_i \cap U_i) \\ &= \sum_{i=1}^{n} d(V_i, U_i) = d(\boldsymbol{V}, \boldsymbol{U}). \end{aligned}$$

4) $d(\boldsymbol{U}, \boldsymbol{W}) \leq d(\boldsymbol{U}, \boldsymbol{V}) + d(\boldsymbol{V}, \boldsymbol{W})$ - Desigualdade Triangular. Seja $\beta = d(\boldsymbol{U}, \boldsymbol{W}) - d(\boldsymbol{U}, \boldsymbol{V}) - d(\boldsymbol{V}, \boldsymbol{W})$. Assim,

$$\begin{aligned} \tfrac{1}{2}(\beta) &= \tfrac{1}{2}(\sum_{i=1}^{n} d(U_i, W_i) - \sum_{i=1}^{n} d(U_i, V_i) - \sum_{i=1}^{n} d(V_i, W_i)) \\ &= \tfrac{1}{2}(\sum_{i=1}^{n} (dim(U_i) + dim(W_i) - 2.dim(U_i \cap W_i)) \\ &- \sum_{i=1}^{n} (dim(U_i) - dim(V_i) + 2.dim(U_i \cap Vi)) \\ &- \sum_{i=1}^{n} (dim(V_i) - dim(W_i) + 2.dim(Vi \cap Wi)) \\ &= \sum_{i=1}^{n} [dim((U_i \cap V_i) + (V_i \cap W_i)) - dim(V_i] \\ &+ \sum_{i=1}^{n} [dim((U_i \cap V_i) \cap (V_i \cap W_i)) - dim(U_i \cap W_i)] \leq 0. \end{aligned}$$

■

Definição 3.3. *Um **código de bloco de subespaços** é um subconjunto não vazio $\boldsymbol{\mathcal{C}} \subset \mathbb{P}(\mathbb{F}_q^m)^n$ e denominado **código de subespaço n-shot**.*

Definição 3.4. *A **cardinalidade do código $\boldsymbol{\mathcal{C}}$** é dada por $\mid \boldsymbol{\mathcal{C}} \mid = M^n$ e a **taxa do código** é definida por $R(\boldsymbol{\mathcal{C}}) = \frac{log\mid\boldsymbol{\mathcal{C}}\mid}{m.n}$ ou $R(\boldsymbol{\mathcal{C}}) = \frac{logM^n}{m.n}$ medida em unidades de informação por uso de canal de subespaço, onde q é a base do logaritmo.*

Definição 3.5. *A **distância mínima** do código $\boldsymbol{\mathcal{C}}$ é definida como:*

$$d = d(\boldsymbol{\mathcal{C}}) = min\{d(\boldsymbol{U}, \boldsymbol{V}),\ \boldsymbol{U},\ \boldsymbol{V} \in \boldsymbol{\mathcal{C}},\ \boldsymbol{U} \neq \boldsymbol{V}\},$$

onde $1 \leq d(\boldsymbol{\mathcal{C}}) \leq mn$ e $0 \leq R(\boldsymbol{\mathcal{C}}) \leq 1$.

Definição 3.6. *Os **parâmetros** do código de subepaço n-shot $\boldsymbol{\mathcal{C}} \subset \mathbb{P}(\mathbb{F}_q^m)^n$ é denotado por $(m.n, M^n, d)$ onde $m.n$ é a dimensão do espaço projetivo, M^n é a cardinalidade do código e d a distância mínima do código. Se o código $\boldsymbol{\mathcal{C}}$ está em uma grassmanniana de dimensão kn os parâmetros do código são (mn, M^n, d, kn).*

Exemplo 3.1. *Considere o espaço projetivo $\mathbb{P}(\mathbb{F}_2^2) \times \mathbb{P}(\mathbb{F}_2^2)$. Sejam $S_1 = WO$, $S_2 = OW$, $S_3 = S_2S_2$ e $S_4 = S_1S_2$ os elementos do Exemplo 2.40 da Seção 2.6. Podemos visualizar na Figura 8 o resultado do Lema 2.1, ou seja, dados dois subespaços de um espaço vetorial de dimensão n, a distância entre eles é máxima se a interseção entre eles é o espaço nulo e a soma das dimensões entre os subespaços é n. Portanto, por meio da Observação 2.29, segue que $WO \oplus OW = WW = \mathbb{F}_2^4$, enquanto que entre WO e S_2S_2 não. Tanto o Lema 2.1 quanto a Observação 2.29 se encontram também na Seção 2.6.*

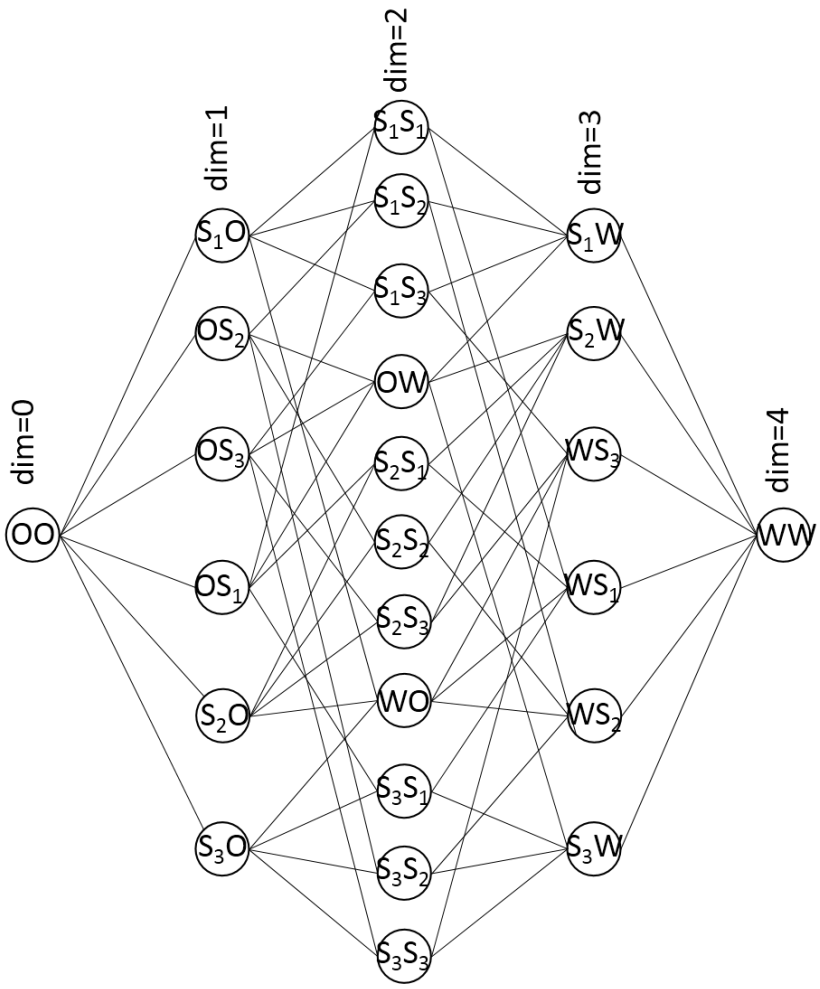


Figura 8 – Espaço Projetivo $\mathbb{P}(\mathbb{F}_2^2) \times \mathbb{P}(\mathbb{F}_2^2)$

Exemplo 3.2. *Considere o espaço projetivo* $\mathbb{P}(\mathbb{F}_2^2) = \{O, S_1, S_2, S_3, W\}$. *Um código de subespaço 2-shot sobre* $\mathbb{P}(\mathbb{F}_2^2) \times \mathbb{P}(\mathbb{F}_2^2)$ *é dado por*

$$\mathcal{C} = \{S_1S_1, S_1S_2, S_1S_3, S_2S_1, S_2S_2, S_2S_3, S_3S_1, S_3S_2, S_3S_3\},$$

onde $S_1 = \{00, 01\},\ S_2 = \{00, 10\},\ S_3 = \{00, 11\}$. *Para este exemplo escolhemos os subespaços que são os elementos do código a ser estendido, de uma mesma grassmanniana. Observe que a distância mínima do código é* $d = 2$, *a menor distância de subespaço entre todas as distâncias obtidas dentre quaisquer duas sequências de subespaços do código. Agora, apresentamos um exemplo do cálculo da distância de subespaço entre duas sequências de subespaços do código. Sejam* $\boldsymbol{U} = (U_1, U_2) = (S_1, S_1)$ *e* $\boldsymbol{V} = (V_1, V_2) = (S_1, S_2)$. *Assim,* $d(\boldsymbol{U}, \boldsymbol{V}) = \sum_{i=1}^{2} d(U_i, V_i) = d(U_1, V_1) + d(U_2, V_2) = dim(S_1) + dim(S_1) - 2.dim(S_1 \cap S_1) + dim(S_1) + dim(S_2) - 2.dim(S_1 \cap S_2) = 1 + 1 - 2 + 1 + 1 - 0 = 2$. *O mesmo cálculo vale para quaisquer dois pares de subespaços do código. Portanto, temos um código de subespaço 2-shot com parâmetros* $(m.n, M^n, d, k.n) = (4, 9, 2, 2)$. *Podemos observar por meio da Figura 8, via os elementos da coluna central, que o código de subespaço 2-shot pertence a uma mesma grassmanniana, neste exemplo, de dimensão 2. Cabe observar, que*

apesar de OW e WO estarem na grassmanniana de dimensão 2, os mesmos não pertencem ao código de subespaço 2-shot, pois não existem subespaços U e V pertencentes a uma grassmanniana, neste caso, de dimensão 1, tal que $UV = OW$ ou $UV = WO$.

Apresentamos, a seguir, um exemplo em que os subespaços que pertencem ao código que será estendido não pertencem a uma mesma grassmanniana, no entanto, daqui em diante consideraremos os códigos que estão em uma mesma grassmanniana.

Exemplo 3.3. *Considere o espaço projetivo $\mathbb{P}(\mathbb{F}_2^3)$. Um código de subespaço 2-shot sobre $\mathbb{P}(\mathbb{F}_2^3) \times \mathbb{P}(\mathbb{F}_2^3)$ é:*

$$\mathcal{C} = \{S_1S_1, S_1S_2, S_1S_3, S_2S_1, S_2S_2, S_2S_3, S_3S_1, S_3S_2, S_3S_3\},$$

onde $S_1 = \{000, 001\}$, $S_2 = \{000, 111\}$, $S_3 = \{000, 100, 010, 110\}$. Observe que a distância mínima do código é $d = 2$, a menor distância de subespaço entre todas as distâncias obtidas dentre quaisquer duas sequências de subespaços do código. A seguir, apresentamos um exemplo do cálculo de distância de subespaço entre duas sequências de subespaços do código. Sejam $\boldsymbol{U} = (U_1, U_2) = (S_1, S_1)$ e $\boldsymbol{V} = (V_1, V_2) = (S_1, S_2)$. Assim $d(\boldsymbol{U}, \boldsymbol{V}) = \sum_{i=1}^{2} d(U_i, V_i) = d(U_1, V_1) + d(U_2, V_2) = dim(S_1) + dim(S_1) - 2.dim(S_1 \cap S_1) + dim(S_1) + dim(S_2) - 2.dim(S_1 \cap S_2) = 1 + 1 - 2 + 1 + 1 - 0 = 2$. O mesmo cálculo vale para quaisquer dois pares de subespaços do código. Portanto, temos um código de subespaço 2-shot com parâmetros $(m.n, M^n, d) = (6, 9, 2)$. Observe que este é um código de subespaço 2-shot que não está em uma mesma Grasmanianna, visto que temos palavras-código em dimensões diferentes, por exemplo, S_1S_1 tem dimensão 2, S_2S_3 tem dimensão 3 e S_3S_3 tem dimensão 4.

3.2 Códigos de Subespaços *n*-shot Geometricamente Uniforme

Nesta seção, apresentamos a definição de códigos de subespaços n-shot geometricamente uniforme e a construção exemplificada por meio de alguns exemplos de códigos de subespaços n-shot $\boldsymbol{\mathcal{C}}$ com essa propriedade, ou seja, dado um grupo de simetrias, cada elemento deste grupo age de forma transitiva nas palavras-código de $\boldsymbol{\mathcal{C}}$.

Definição 3.7. *Uma isometria T do espaço métrico $(\mathbb{P}(\mathbb{F}_q^m), d)$ é uma **transformação** $T : \mathbb{P}(\mathbb{F}_q^m) \to \mathbb{P}(\mathbb{F}_q^m)$ que preserva a distância de subespaço d, ou seja, $d(T(U), T(V)) = d(U, V)$, para todo $U, V \in \mathbb{P}(\mathbb{F}_q^m)$.*

Definição 3.8. *Um **código de subespaço $\mathcal{C}$ é geometricamente uniforme** se dado quaisquer dois subespaços $U, V \in \mathcal{C}$ existe uma isometria I tal que:*

- $I(U) = V$

- $I(\mathcal{C}) = \mathcal{C}$

A seguir, apresentamos alguns fatos sobre isometria:

- A função identidade é uma isometria.
- A inversa de uma isometria é uma isometria.
- A composição de duas isometrias é também uma isometria.

Lema 3.1. *A transformação* $T_{ij} : \mathcal{C} \subseteq \mathbb{P}(\mathbb{F}_q^m) \to \mathcal{C} \subseteq \mathbb{P}(\mathbb{F}_q^m)$ *definida por:*

$$\begin{cases} T_{ij}(U_i) = U_j \\ T_{ji}(U_j) = U_i \\ T_{ij}(U_k) = U_k, \end{cases} \tag{3.2}$$

$k \neq i, j$ *é uma isometria para quaisquer* $i, j \in \{1, \cdots, n\}$.

Lema 3.2. *O código* $\mathcal{C}$ *é um código de subespaço geometricamente uniforme com a isometria* T_{ij} *estabelecida no Lema 3.1.*

Os Lemas 3.1 e 3.2 estão demonstrados em (MIYAMOTO, 2015).

Definição 3.9. *Um* ***código de subespaço n-shot*** $\boldsymbol{\mathcal{C}}$ ***é geometricamente uniforme*** *se dado quaisquer dois vetores de subespaços* $\boldsymbol{U}, \boldsymbol{V} \in \boldsymbol{\mathcal{C}}$ *existe uma isometria I tal que:*

- $I(\boldsymbol{U}) = \boldsymbol{V}$,
- $I(\boldsymbol{\mathcal{C}}) = \boldsymbol{\mathcal{C}}$.

Lema 3.3. *A transformação,*

$$T_{ij} : \boldsymbol{\mathcal{C}} = \overbrace{\mathcal{C} \times \mathcal{C} \times \cdots \times \mathcal{C}}^{n-vezes} \subseteq \mathbb{P}(\mathbb{F}_q^m)^n \to \boldsymbol{\mathcal{C}} = \overbrace{\mathcal{C} \times \mathcal{C} \times \cdots \times \mathcal{C}}^{n-vezes} \subseteq \mathbb{P}(\mathbb{F}_q^m)^n,$$

onde o código de subespaço $\boldsymbol{\mathcal{C}}$ *é o produto cartesiano n-vezes do código de subespaço* $\mathcal{C}$*, definida por:*

$$\begin{cases} T_{ij}(\boldsymbol{U}_i) = \boldsymbol{U}_j \\ T_{ji}(\boldsymbol{U}_j) = \boldsymbol{U}_i \\ T_{ij}(\boldsymbol{U}_k) = \boldsymbol{U}_k, \end{cases} \tag{3.3}$$

$k \neq i, j$ *é uma isometria para quaiquer* $i, j \in \{1, \cdots, n\}$.

Lema 3.4. *O código* $\boldsymbol{\mathcal{C}}$ *é um código de subespaço n-shot geometricamente uniforme com a isometria* T_{ij} *estabelecida no Lema 3.3.*

Apresentamos, a seguir, alguns resultados algébricos, que podem ser encontrados para maiores detalhes em (ROTMAN, 1993), com o objetivo de utilizá-los na fundamentação matemática da construção dos códigos de subespaços n-shot geometricamente uniforme.

Teorema 3.2. *Sejam $G_1, G_2, \cdots, G_n$, grupos. Para $(a_1, a_2, a_3, \cdots, a_n)$ e $(b_1, b_2, b_3, \cdots, b_n)$ em $\prod_{i=1}^{n} G_i$, defina $(a_1, a_2, a_3, \cdots, a_n).(b_1, b_2, b_3, \cdots, b_n) = (a_1b_1, a_2b_2, a_3b_3, \cdots, a_nb_n)$. Então, $\prod_{i=1}^{n} G_i$ é um grupo, isto é, o produto direto dos grupos G_i, denotado por $G = G_1 \times G_2 \cdots \times G_n$, sob esta operação binária.*

Definição 3.10. *Se G é um p-grupo abeliano para algum primo p, então G é chamado* ***grupo p-primário****.*

Teorema 3.3. *(**Decomposição Primária**) Um grupo abeliano finito G é uma soma direta de grupos p-primários.*

Teorema 3.4. *Um grupo abeliano finito G é uma soma direta de grupos cíclicos.*

A seguir, apresentamos vários exemplos da construção de códigos de subespaços n-shot geometricamente uniforme, com o objetivo de facilitar a fixação da técnica utilizada para a construção. Tal técnica está justificada principalmente na utilização dos Teoremas 3.3 e 3.4.

Exemplo 3.4. *Neste exemplo, consideramos a construção dos códigos de subespaço 1-shot, 2-shot e 3-shot geometricamente uniforme. Para isso, considere o espaço projetivo $\mathbb{P}(\mathbb{F}_2^2)$.*

- *O código de subespaço 1-shot $\mathcal{C}_1^{(1)}$ é especificado por $\mathcal{C}_1^{(1)} = \{S_1, S_2\}$, onde $S_1 = \{00, 10\}$ e $S_2 = \{00, 01\}$. Considerando $P_0 = [1 \quad 0]$ a matriz geradora de S_1 e $P_1 = [0 \quad 1]$ a matriz geradora de S_2, então existe um subgrupo abeliano, neste caso, um subgrupo cíclico Q_1, dado por:*

$$Q_1 = \left\{ Q_1^{(1)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, Q_2^{(1)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}.$$

  Neste caso, é o grupo das permutações que age transitivamente nas palavras-código de $\mathcal{C}_1^{(1)}$, onde $Q_j^{(i)}$ são elementos do grupo para j variando dentro da cardinalidade do código e i associado à n-ésima extensão do código, ou seja:

$$P_0.Q_1^{(1)} = P_0 \qquad [1 \quad 0].\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = [1 \quad 0]$$

e

$$P_0.Q_2^{(1)} = P_1 \qquad [1 \quad 0].\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = [0 \quad 1]$$

ou

$$P_1.Q_1^{(1)} = P_0 \qquad [0 \quad 1].\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = [0 \quad 1]$$

e

$$P_1.Q_2^{(1)} = P_1 \qquad [0 \quad 1].\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = [1 \quad 0].$$

Portanto, $\mathcal{C}_1^{(1)}$ *é um código de subespaço 1-shot geometricamente uniforme com parâmetros* $(m, M, d, k) = (2, 2, 2, 1)$*, cuja taxa do código é* $R(\mathcal{C}_1^{(1)}) = \frac{log_2 2^1}{2 \cdot 1} = \frac{1}{2} = 0,5$.

- *A extensão do código* $\mathcal{C}_1^{(1)}$ *para o caso código de subespaço 2-shot* $\boldsymbol{\mathcal{C}}_1^{(2)}$*, é dada por* $\boldsymbol{\mathcal{C}}_1^{(2)} = \mathcal{C}_1^{(1)} \times \mathcal{C}_1^{(1)} = \{S_1, S_2\} \times \{S_1, S_2\} = \{S_1S_1, S_1S_2, S_2S_1, S_2S_2\}$ *onde,*

$$\begin{aligned} S_1S_1 &= \{0000, 0010, 1000, 1010\} = \langle 0010, 1000\rangle, \\ S_1S_2 &= \{0000, 0001, 1000, 1001\} = \langle 0001, 1000\rangle, \\ S_2S_1 &= \{0000, 0010, 0100, 0110\} = \langle 0010, 0100\rangle, \\ S_2S_2 &= \{0000, 0001, 0100, 0101\} = \langle 0001, 0100\rangle. \end{aligned}$$

Neste caso, $\langle e_1, e_2, \cdots, e_k\rangle$ *denota os geradores canônicos do subespaço. As matrizes* P_0, P_1,
P_2, P_3 *são matrizes compostas pelos geradores nas linhas, dos respectivos subespaços acima, isto é,*

$$P_0 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \text{ gera } S_1S_1, \quad P_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \text{ gera } S_1S_2.$$

$$P_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \text{ gera } S_2S_1. \quad P_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \text{ gera } S_2S_2.$$

Por meio dos Teoremas 3.3 e 3.4, obtemos os seguintes elementos de um subgrupo abeliano do grupo das permutações, da seguinte maneira:

$$\begin{aligned} Q_1^{(2)} &= Q_1^{(1)} \times Q_1^{(1)} \equiv Q_1^{(1)} \oplus Q_1^{(1)}, \\ Q_2^{(2)} &= Q_1^{(1)} \times Q_2^{(1)} \equiv Q_1^{(1)} \oplus Q_2^{(1)}, \\ Q_3^{(2)} &= Q_2^{(1)} \times Q_1^{(1)} \equiv Q_2^{(1)} \oplus Q_1^{(1)}, \\ Q_4^{(2)} &= Q_2^{(1)} \times Q_2^{(1)} \equiv Q_2^{(1)} \oplus Q_2^{(1)}, \end{aligned}$$

tal que:

- $P_iQ_1^{(2)} = P_i$,

– $P_iQ_2^{(2)} = P_{(i+1)mod\ 4}$
– $P_iQ_3^{(2)} = P_{(i+2)mod\ 4}$
– $P_iQ_4^{(2)} = P_{(i+3)mod\ 4}$

para qualquer $i \in \{0,1,2,3\}$*, onde a representação matricial de* Q_2 *é dada por:*

$$Q_2 = \left\{ Q_1^{(2)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, Q_2^{(2)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, Q_3^{(2)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \right.$$

$$\left. Q_4^{(2)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \right\}.$$

Assim, como cada elemento do grupo Q_2 *age transitivamente nos elementos do código de subespaço 2-shot* $\boldsymbol{\mathcal{C}}_1^{(2)}$*, segue que* $\boldsymbol{\mathcal{C}}_1^{(2)}$ *é um código de subespaço 2-shot geometricamente uniforme com parâmetros* $(m.n, M^n, d, k.n) = (4, 4, 2, 2)$*, onde a taxa do código* $R(\boldsymbol{\mathcal{C}}_1^{(2)}) = \frac{log_2 4^2}{4 \cdot 2} = \frac{log_2 2^4}{8} = \frac{1}{2} = 0,5$.

- *Para o caso do código de subespaço 3-shot* $\boldsymbol{\mathcal{C}}_1^{(3)}$*, temos:*

$$\boldsymbol{\mathcal{C}}_1^{(3)} = \{S_1, S_2\} \times \{S_1, S_2\} \times \{S_1, S_2\}$$
$$= \{S_1S_1S_1, S_1S_1S_2, S_1S_2S_1, S_1S_2S_2, S_2S_1S_1, S_2S_1S_2, S_2S_2S_1, S_2S_2S_2\},$$

onde as palavras-código, são:

$$S_1S_1S_1 = \langle 000010, 001000, 100000 \rangle,$$
$$S_1S_1S_2 = \langle 000001, 001000, 100000 \rangle,$$
$$S_1S_2S_1 = \langle 000010, 000100, 100000 \rangle,$$
$$S_1S_2S_2 = \langle 000001, 000100, 100000 \rangle,$$
$$S_2S_1S_1 = \langle 000010, 001000, 010000 \rangle,$$
$$S_2S_1S_2 = \langle 000001, 001000, 010000 \rangle,$$
$$S_2S_2S_1 = \langle 000010, 000100, 010000 \rangle,$$
$$S_2S_2S_2 = \langle 000001, 000100, 010000 \rangle.$$

As matrizes $P_0, P_1, \cdots, P_7$ *são compostas pelos geradores dos respectivos subespaços, dadas por*

$$P_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, P_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \cdots, P_7 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Novamente, pelos Teoremas 3.3 e 3.4 obtemos o subgrupo abeliano $Q_3 = \{Q_1^{(3)}, \cdots, Q_8^{(3)}\}$ *do grupo das permutações, cujos elementos são:*

$$\begin{aligned}
Q_1^{(3)} &= Q_1^{(1)} \times Q_1^{(1)} \times Q_1^{(1)} \equiv Q_1^{(1)} \oplus Q_1^{(1)} \oplus Q_1^{(1)},\\
Q_2^{(3)} &= Q_1^{(1)} \times Q_1^{(1)} \times Q_2^{(1)} \equiv Q_1^{(1)} \oplus Q_1^{(1)} \oplus Q_2^{(1)},\\
Q_3^{(3)} &= Q_1^{(1)} \times Q_2^{(1)} \times Q_1^{(1)} \equiv Q_1^{(1)} \oplus Q_2^{(1)} \oplus Q_1^{(1)},\\
Q_4^{(3)} &= Q_1^{(1)} \times Q_2^{(1)} \times Q_2^{(1)} \equiv Q_1^{(1)} \oplus Q_2^{(1)} \oplus Q_2^{(1)},\\
Q_5^{(3)} &= Q_2^{(1)} \times Q_1^{(1)} \times Q_1^{(1)} \equiv Q_2^{(1)} \oplus Q_1^{(1)} \oplus Q_1^{(1)},\\
Q_6^{(3)} &= Q_2^{(1)} \times Q_1^{(1)} \times Q_2^{(1)} \equiv Q_2^{(1)} \oplus Q_1^{(1)} \oplus Q_2^{(1)},\\
Q_7^{(3)} &= Q_2^{(1)} \times Q_2^{(1)} \times Q_1^{(1)} \equiv Q_2^{(1)} \oplus Q_2^{(1)} \oplus Q_1^{(1)},\\
Q_8^{(3)} &= Q_2^{(1)} \times Q_2^{(1)} \times Q_2^{(1)} \equiv Q_2^{(1)} \oplus Q_2^{(1)} \oplus Q_2^{(1)}.
\end{aligned}$$

Os elementos do grupo Q_3 *agem transitivamente nos elementos do código* $\boldsymbol{\mathcal{C}}_1^{(3)}$ *da seguinte maneira:*

- $P_i Q_1^{(3)} = P_i$,
- $P_i Q_2^{(3)} = P_{(i+1) mod\ 8}$
- $P_i Q_3^{(3)} = P_{(i+2) mod\ 8}$
- $P_i Q_4^{(3)} = P_{(i+3) mod\ 8}$
- $P_i Q_5^{(3)} = P_{(i+4) mod\ 8}$
- $P_i Q_6^{(3)} = P_{(i+5) mod\ 8}$
- $P_i Q_7^{(3)} = P_{(i+6) mod\ 8}$
- $P_i Q_8^{(3)} = P_{(i+7) mod\ 8}$

para qualquer $i \in \{0, 1, 2, 3, 4, 5, 6, 7\}$. *Com isso, segue que* $\boldsymbol{\mathcal{C}}_1^{(3)}$ *é um código de subespaço 3-shot geometricamente uniforme com parâmetros* $(m.n, M^n, d, k.n) = (6, 8, 2, 3)$, *onde a taxa do código é* $R(\boldsymbol{\mathcal{C}}_1^{(3)}) = \frac{log_2 8^3}{6 \cdot 3} = \frac{log_2 2^9}{18} = \frac{1}{2} = 0,5$.

Exemplo 3.5. *Considere o espaço projetivo* $\mathbb{P}(\mathbb{F}_2^3)$. *Neste exemplo, apresentamos a construção dos códigos de subespaço 1-shot, 2-shot geometricamente uniforme.*

- *O código de subespaço 1-shot* $\mathcal{C}_2^{(1)} = \{S_1, S_2, S_3\}$, *onde as palavras-código são:*

$$\begin{aligned}
S_1 &= \{000, 100, 010, 110\},\\
S_2 &= \{000, 010, 001, 011\}\\
S_3 &= \{000, 001, 100, 101\}
\end{aligned}$$

é geometricamente uniforme. De fato:

Considere a matriz $P_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ *que gera* S_1*, a matriz* $P_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ *que gera* S_2 *e a matriz* $P_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ *que gera* S_3*.*

Neste caso, existe um subgrupo abeliano,

$$Q_1 = \left\{ \sigma_0 = (123) = Q_1^{(1)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \sigma_1 = (312) = Q_2^{(1)} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \right.$$
$$\left. \sigma_2 = (231) = Q_3^{(1)} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \right\},$$

que neste caso, é um subrgrupo cíclico do grupo das permutações de ordem 3, tal que:

- $P_i Q_1^{(1)} = P_i$
- $P_i Q_2^{(1)} = P_{(i+1) mod\ 3}$
- $P_i Q_3^{(1)} = P_{(i+2) mod\ 3}$

para qualquer $i \in \{0, 1, 2\}$*. Portanto,* $\mathcal{C}_2^{(1)}$ *é um código de subespaço 1-shot geometricamente uniforme com parâmetros* $(m, M, d, k) = (3, 3, 2, 2)$*, onde a taxa do código é* $R(\mathcal{C}_2^{(1)}) = \frac{log_2 3^1}{3 \cdot 1} = \frac{1{,}58496}{3} = 0,52832$*.*

- *A extensão do código de subespaço* $\mathcal{C}_2^{(1)}$ *para o código de subespaço 2-shot* $\boldsymbol{\mathcal{C}_2^{(2)}}$

  $\boldsymbol{\mathcal{C}_2^{(2)}} = \mathcal{C}_2^{(1)} \times \mathcal{C}_2^{(1)} = \{S_1S_1, S_1S_2, S_1S_3, S_2S_1, S_2S_2, S_2S_3, S_3S_1, S_3S_2, S_3S_3\}$*, onde:*

$$\begin{aligned}
S_1S_1 &= \langle 000100, 000010, 100000, 010000 \rangle, \\
S_1S_2 &= \langle 000010, 000001, 100000, 010000 \rangle, \\
S_1S_3 &= \langle 000001, 000100, 100000, 010000 \rangle, \\
S_2S_1 &= \langle 000100, 000010, 010000, 001000 \rangle, \\
S_2S_2 &= \langle 000010, 000001, 010000, 001000 \rangle, \\
S_2S_3 &= \langle 000001, 000100, 010000, 001000 \rangle, \\
S_3S_1 &= \langle 000100, 000010, 001000, 100000 \rangle, \\
S_3S_2 &= \langle 000010, 000001, 001000, 100000 \rangle, \\
S_3S_3 &= \langle 000001, 000100, 001000, 100000 \rangle
\end{aligned}$$

$$P_0 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ gera } S_1S_1, \quad P_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ gera } S_1S_2,$$

$$P_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \textit{ gera } S_1S_3, \quad P_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \textit{ gera } S_2S_1,$$

$$P_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \textit{ gera } S_2S_2, \quad P_5 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \textit{ gera } S_2S_3,$$

$$P_6 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \textit{ gera } S_3S_1, \quad P_7 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \textit{ gera } S_3S_2,$$

$$P_8 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \textit{ gera } S_3S_3.$$

Através dos Teoremas 3.3 e 3.4 obtemos um subrgrupo abeliano $Q_2 = \{Q_1^{(2)}, Q_2^{(2)}, Q_3^{(2)}, Q_4^{(2)}, Q_5^{(2)}, Q_6^{(2)}, Q_7^{(2)}, Q_8^{(2)}, Q_9^{(2)}\}$, *onde cada elemento é representado por uma matriz* 6×6, *obtida através das igualdades:*

$$\begin{aligned} Q_1^{(2)} &= Q_1^{(1)} \times Q_1^{(1)} \equiv Q_1^{(1)} \oplus Q_1^{(1)}, \\ Q_2^{(2)} &= Q_1^{(1)} \times Q_2^{(1)} \equiv Q_1^{(1)} \oplus Q_2^{(1)}, \\ Q_3^{(2)} &= Q_1^{(1)} \times Q_3^{(1)} \equiv Q_1^{(1)} \oplus Q_3^{(1)}, \\ Q_4^{(2)} &= Q_2^{(1)} \times Q_1^{(1)} \equiv Q_2^{(1)} \oplus Q_1^{(1)}, \\ Q_5^{(2)} &= Q_2^{(1)} \times Q_2^{(1)} \equiv Q_2^{(1)} \oplus Q_2^{(1)}, \\ Q_6^{(2)} &= Q_2^{(1)} \times Q_3^{(1)} \equiv Q_2^{(1)} \oplus Q_3^{(1)}, \\ Q_7^{(2)} &= Q_3^{(1)} \times Q_1^{(1)} \equiv Q_3^{(1)} \oplus Q_1^{(1)}, \\ Q_8^{(2)} &= Q_3^{(1)} \times Q_2^{(1)} \equiv Q_3^{(1)} \oplus Q_2^{(1)}, \\ Q_9^{(2)} &= Q_3^{(1)} \times Q_3^{(1)} \equiv Q_3^{(1)} \oplus Q_3^{(1)} \end{aligned}$$

cujos elementos do grupo Q_2 *agem transitivamente sobre os elementos do código* $\boldsymbol{\mathcal{C}_2^{(2)}}$, *da seguinte maneira:*

- $P_i Q_1^{(2)} = P_i$
- $P_i Q_2^{(2)} = P_{(i+1) mod\ 9}$

- $P_iQ_3^{(2)} = P_{(i+2)mod\ 9}$
- $P_iQ_4^{(2)} = P_{(i+3)mod\ 9}$
- $P_iQ_5^{(2)} = P_{(i+4)mod\ 9}$
- $P_iQ_6^{(2)} = P_{(i+5)mod\ 9}$
- $P_iQ_7^{(2)} = P_{(i+6)mod\ 9}$
- $P_iQ_8^{(2)} = P_{(i+7)mod\ 9}$
- $P_iQ_9^{(2)} = P_{(i+8)mod\ 9}$

para qualquer $i \in \{0,1,2,3,4,5,6,7,8\}$. *Portanto,* $\boldsymbol{\mathcal{C}_2^{(2)}}$ *é um código de subespaço 2-shot geometricamente uniforme com parâmetros* $(m.n, M^n, d, k.n) = (6, 9, 2, 4)$, *cuja taxa do código é* $R(\boldsymbol{\mathcal{C}_2^{(2)}}) = \frac{log_2 9^2}{6\cdot 2} = \frac{log_2 3^4}{12} = \frac{6{,}33984}{12} = 0,52832$.

Exemplo 3.6. *Considere o espaço projetivo* $\mathbb{P}(\mathbb{F}_2^4)$. *Para este exemplo, consideramos a construção dos códigos de subespaço 1-shot, 2-shot geometricamente uniforme.*

- *O código de subespaço 1-shot* $\mathcal{C}_3^{(1)} = \{S_1, S_2, S_3, S_4\}$, *onde:*

$$S_1 = \{0000, 1000, 0100, 0010, 1100, 1010, 0110, 1110\} = \langle 1000, 0100, 0010\rangle,$$
$$S_2 = \{0000, 0100, 0010, 0001, 0110, 0101, 0011, 0111\} = \langle 0100, 0010, 0001\rangle,$$
$$S_3 = \{0000, 0100, 0001, 1000, 0011, 1010, 1001, 1011\} = \langle 0010, 0001, 1000\rangle$$
$$S_4 = \{0000, 0001, 1000, 0100, 1001, 0101, 1100, 1101\} = \langle 0001, 1000, 0100\rangle.$$

é geometricamente uniforme. De fato:

$$P_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, P_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, P_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}, P_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Existe um subgrupo abeliano,

$$Q_1 = \left\{ Q_1^{(1)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, Q_2^{(1)} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, Q_3^{(1)} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \right.$$
$$\left. Q_4^{(1)} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \right\},$$

tal que:

- $P_i.Q_1^{(i)} = P_i$
- $P_i.Q_2^{(i)} = P_{(i+1)mod\ 4}$
- $P_i.Q_3^{(i)} = P_{(i+2)mod\ 4}$
- $P_i.Q_4^{(i)} = P_{(i+3)mod\ 4}$

para qualquer $i \in \{0,1,2,3\}$. *Portanto,* $\mathcal{C}_3^{(1)}$ *é um código de subespaço 1-shot geometricamente uniforme com parâmetros* $(m, M, d, k) = (4, 4, 2, 3)$, *onde a taxa do código é dada por* $R(\mathcal{C}_3^{(1)}) = \frac{log_2 4^1}{4 \cdot 1} = \frac{1}{2} = 0,5$.

- *A extensão do código* $\mathcal{C}_3^{(1)}$ *para o código de subespaço 2-shot* $\boldsymbol{\mathcal{C}_3^{(2)}}$, *é dada por*

$$\boldsymbol{\mathcal{C}_3^{(2)}} = \mathcal{C}_3^{(1)} \times \mathcal{C}_3^{(1)} = \{S_1S_1, S_1S_2, S_1S_3, S_1S_4, S_2S_1, S_2S_2, S_2S_3, S_2S_4, S_3S_1, S_3S_2, S_3S_3, S_3S_4, S_4S_1, S_4S_2, S_4S_3, S_4S_4\}.$$

Considere as seguintes matrizes $P_0, P_1, \cdots, P_{15}$, *compostas pelos geradores nas linhas, que geram os subespaços* $S_1S_1, S_1S_2, \cdots, S_4S_4$, *respectivamente:*

$$P_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \cdots, P_{15} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Através dos Teoremas 3.3 e 3.4 obtemos um subrgrupo abeliano $Q_2 = \{Q_1^{(2)}, \cdots, Q_7^{(2)}, Q_8^{(2)}, \cdots, Q_{16}^{(2)}\}$, *onde cada elemento é representado por uma matriz* 8×8, *obtida das seguintes igualdades:*

$$\begin{aligned}
Q_1^{(2)} &= Q_1^{(1)} \times Q_1^{(1)} \equiv Q_1^{(1)} \oplus Q_1^{(1)}, \\
Q_2^{(2)} &= Q_1^{(1)} \times Q_2^{(1)} \equiv Q_1^{(1)} \oplus Q_2^{(1)}, \\
Q_3^{(2)} &= Q_1^{(1)} \times Q_3^{(1)} \equiv Q_1^{(1)} \oplus Q_3^{(1)}, \\
Q_4^{(2)} &= Q_1^{(1)} \times Q_4^{(1)} \equiv Q_1^{(1)} \oplus Q_4^{(1)}, \\
Q_5^{(2)} &= Q_2^{(1)} \times Q_1^{(1)} \equiv Q_2^{(1)} \oplus Q_1^{(1)}, \\
Q_6^{(2)} &= Q_2^{(1)} \times Q_2^{(1)} \equiv Q_2^{(1)} \oplus Q_2^{(1)}, \\
Q_7^{(2)} &= Q_2^{(1)} \times Q_3^{(1)} \equiv Q_2^{(1)} \oplus Q_3^{(1)}, \\
Q_8^{(2)} &= Q_2^{(1)} \times Q_4^{(1)} \equiv Q_2^{(1)} \oplus Q_4^{(1)}, \\
Q_9^{(2)} &= Q_3^{(1)} \times Q_1^{(1)} \equiv Q_3^{(1)} \oplus Q_1^{(1)}, \\
Q_{10}^{(2)} &= Q_3^{(1)} \times Q_2^{(1)} \equiv Q_3^{(1)} \oplus Q_2^{(1)}, \\
Q_{11}^{(2)} &= Q_3^{(1)} \times Q_3^{(1)} \equiv Q_3^{(1)} \oplus Q_3^{(1)},
\end{aligned}$$

$$Q_{12}^{(2)} = Q_3^{(1)} \times Q_4^{(1)} \equiv Q_3^{(1)} \oplus Q_4^{(1)},$$
$$Q_{13}^{(2)} = Q_4^{(1)} \times Q_1^{(1)} \equiv Q_4^{(1)} \oplus Q_1^{(1)},$$
$$Q_{14}^{(2)} = Q_4^{(1)} \times Q_2^{(1)} \equiv Q_4^{(1)} \oplus Q_2^{(1)},$$
$$Q_{15}^{(2)} = Q_4^{(1)} \times Q_3^{(1)} \equiv Q_4^{(1)} \oplus Q_3^{(1)},$$
$$Q_{16}^{(2)} = Q_4^{(1)} \times Q_4^{(1)} \equiv Q_4^{(1)} \oplus Q_4^{(1)}.$$

Cada elemento do grupo Q_2 age transitivamente sobre as palavras-código de $\boldsymbol{\mathcal{C}_3^{(2)}}$, da seguinte forma:

- $P_i.Q_1^{(2)} = P_i$
- $P_i.Q_2^{(2)} = P_{(i+1)mod\ 16}$

  $\vdots$

- $P_i.Q_{16}^{(2)} = P_{(i+15)mod\ 16}$

Logo, $\boldsymbol{\mathcal{C}_3^{(2)}}$ é um código de subespaço 2-shot geometricamente uniforme com parâmetros $(m.n, M^n, d, k.n) = (8, 16, 2, 6)$, onde a taxa do código é dada por $R(\boldsymbol{\mathcal{C}_3^{(2)}}) = \frac{log_2 16^2}{8 \cdot 2} = \frac{log_2 2^8}{16} = \frac{1}{2} = 0,5$.

Exemplo 3.7. *Para este exemplo, consideramos a construção dos códigos de subespaço 1-shot, 2-shot geometricamente uniforme. Neste caso, considere o espaço projetivo $\mathbb{P}(\mathbb{F}_2^7)$.*

- *O código $\mathcal{C}_4^{(1)} = \{S_1, S_2, S_3, S_4, S_5, S_6, S_7\}$, onde:*

$$S_1 = \langle 1000000, 0100000, 0001000 \rangle,$$
$$S_2 = \langle 0100000, 0010000, 0000100 \rangle,$$
$$S_3 = \langle 0010000, 0001000, 0000010 \rangle,$$
$$S_4 = \langle 0001000, 0000100, 0000001 \rangle,$$
$$S_5 = \langle 0000100, 0000010, 1000000 \rangle,$$
$$S_6 = \langle 0000010, 0000001, 0100000 \rangle,$$
$$S_7 = \langle 0000001, 1000000, 0010000 \rangle.$$

é geometricamente uniforme. De fato: Considere as seguintes matrizes, compostas pelos geradores dos subespaços $S_1, \cdots, S_7$ nas linhas:

$$P_0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}, \cdots, P_6 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Neste caso, existe um subgrupo abeliano do grupo das permutações onde cada elemento desse grupo atua transitivamente no código $C_4^{(1)}$

$$Q_1 = \left\{ Q_1^{(1)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \cdots, Q_7^{(1)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \right\},$$

tal que:

- $P_i.Q_1^{(i)} = P_i$
- $P_i.Q_2^{(i)} = P_{(i+1)mod\ 7}$
- $P_i.Q_3^{(i)} = P_{(i+2)mod\ 7}$
- $P_i.Q_4^{(i)} = P_{(i+3)mod\ 7}$
- $P_i.Q_5^{(i)} = P_{(i+4)mod\ 7}$
- $P_i.Q_6^{(i)} = P_{(i+5)mod\ 7}$
- $P_i.Q_7^{(i)} = P_{(i+6)mod\ 7}$

para qualquer $i \in \{0, 1, 2, 3, 4, 5, 6\}$.
Portanto, $\mathcal{C}_4^{(1)}$ *é um código de subespaço 1-shot geometricamente uniforme com parâmetros* $(m, M, d, k) = (7, 7, 4, 3)$*, cuja taxa do código é* $R(\mathcal{C}_4^{(1)}) = \frac{log_2 7^1}{7 \cdot 1} = \frac{2{,}80735}{7} = 0{,}40105$.

- *A extensão do código* $\mathcal{C}_4^{(1)}$ *para o código de subespaço 2-shot* $\boldsymbol{\mathcal{C}_4^{(2)}}$*, é dada por* $\boldsymbol{\mathcal{C}_4^{(2)}} = \mathcal{C}_4^{(1)} \times \mathcal{C}_4^{(1)} = \{S_1S_1, S_1S_2, S_1S_3, \cdots, S_7S_7\}$*, onde a cardinalidade do código* $\boldsymbol{\mathcal{C}_4^{(2)}}$ *é 49. Considere:*

$$P_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad gera \quad S_1S_1,$$

$$\vdots$$

$$P_{48} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad gera \quad S_7S_7.$$

Através dos Teoremas 3.3 e 3.4 obtemos um subrgrupo abeliano $Q_2 = \{Q_1^{(2)}, \cdots, Q_{25}^{(2)}, Q_{26}^{(2)}, \cdots, Q_{49}^{(2)}\}$*, onde cada elemento é representado por uma matriz* 14×14*, tal que:*

$$\begin{aligned} Q_1^{(2)} &= Q_1^{(1)} \times Q_1^{(1)} \equiv Q_1^{(1)} \oplus Q_1^{(1)}, \\ Q_2^{(2)} &= Q_1^{(1)} \times Q_2^{(1)} \equiv Q_1^{(1)} \oplus Q_2^{(1)}, \\ &\vdots \\ Q_7^{(2)} &= Q_1^{(1)} \times Q_7^{(1)} \equiv Q_1^{(1)} \oplus Q_7^{(1)}, \\ Q_8^{(2)} &= Q_2^{(1)} \times Q_1^{(1)} \equiv Q_2^{(1)} \oplus Q_1^{(1)}, \\ &\vdots \\ Q_{49}^{(2)} &= Q_7^{(1)} \times Q_7^{(1)} \equiv Q_7^{(1)} \oplus Q_7^{(1)} \end{aligned}$$

cujos elementos do grupo Q_2 *agem transitivamente sobre as palavras-código de* $\boldsymbol{\mathcal{C}_4^{(2)}}$*, da seguinte forma:*

- $P_i.Q_1^{(2)} = P_i$
- $P_i.Q_2^{(2)} = P_{(i+1)mod\ 49}$

  $\vdots$

- $P_i.Q_{49}^{(2)} = P_{(i+48)mod\ 49}$.

Portanto, $\boldsymbol{\mathcal{C}_4^{(2)}}$ *é um código de subespaço 2-shot geometricamente uniforme com parâmetros* $(m.n, M^n, d, k.n) = (14, 49, 4, 6)$*, onde a taxa do código é dada por* $R(\boldsymbol{\mathcal{C}_4^{(2)}}) = \frac{log_2 49^2}{14 \cdot 2} = \frac{2{,}80735}{7} = 0,40105$.

Observação 3.1. *Como pode ser observado nos exemplos anteriores as taxas dos códigos permanecem inalteradas a medida que usamos várias vezes o canal.*

Os Exemplos 3.4, 3.5, 3.6 e 3.7 conduzem ao estabelecimento do que venha a ser um código de subespaço n-shot geometricamente uniforme.

Definição 3.11. *Seja* $\mathcal{C} = \{S_1, S_2, \cdots, S_M\}$ *um código de subespaço 1-shot. Dizemos que* $\mathcal{C}$ *é um* ***código de subespaço 1-shot geometricamente uniforme*** *com parâmetros* (m, M, d, k) *para algum espaço projetivo* $\mathbb{P}(\mathbb{F}_2^m)$ *conveniente, se existe um subgrupo abeliano* $Q_1 = \{Q_1^{(1)}, Q_2^{(1)}, \cdots, Q_M^{(1)}\}$*, tal que os elementos de* Q_1 *agem transitivamente sobre os subespaços de* $\mathcal{C}$*, representados pelas matrizes* $P_0, P_1, \cdots, P_M$*, ou seja,* $P_iQ_1 = P_i, P_iQ_2 = P_{(i+1)mod\ M}, \cdots, P_iQ_M = P_{(i+(M-1))mod\ M}$.

Proposição 3.1. *Seja a n-ésima extensão do código* $\mathcal{C}$*, dada por,* $\boldsymbol{\mathcal{C}} = \mathcal{C} \times \mathcal{C} \times \cdots \times \mathcal{C}$ *e a n-ésima extensão do espaço projetivo* $\mathbb{P}(\mathbb{F}_q^m)$*, como sendo,* $\mathbb{P}(\mathbb{F}_q^m)^n$*. O código* $\boldsymbol{\mathcal{C}}$ *é um* ***código de subespaço n-shot geometricamente uniforme*** *em* $\mathbb{P}(\mathbb{F}_q^m)^n$ *com parâmetros* $(m.n, M^n, d, k.n)$*. Nestas condições, existe um subgrupo abeliano* $Q_n = \{Q_1^{(n)}, Q_2^{(n)}, \cdots, Q_{M^n}^{(n)}\}$,

onde cada $Q_i^{(n)}$ *para* $i \in \{1, 2, \cdots, M^n\}$ *é a soma direta de combinações de elementos de* Q_1*, que agem transitivamente nas matrizes geradoras* $P_0, P_1, \cdots, P_{M^n}$*, da seguinte forma* $P_i Q_1^{(n)} = P_i, P_i Q_2^{(n)} = P_{(i+1) mod\ M^n}, \cdots, P_i Q_{M^n}^{(n)} = P_{(i+(M^n-1)) mod\ M^n}$.

4 Isomorfismo entre Reticulados de Grupos e Espaços Projetivos

Neste capítulo, apresentamos uma relação existente entre classes de espaços projetivos e uma estrutura algébrica com objetivo de fornecer elementos que possam serem úteis para a construção de códigos de subespaços, especialmente, códigos de subespaços n-shot (STINSON, 2004; COULBORN; DINITZ, 2007; LIMA; PALAZZO, 2017b). Na seção 4.1, apresentamos, através de alguns exemplos, relações existentes entre design combinatório e espaços projetivos através do diagrama de Hasse desses espaços projetivos. Na Seção 4.2, apresentamos uma proposta de estrutura algébrica e mostramos um isomorfismo existente entre o reticulado de um grupo abeliano consistindo do produto direto de grupos abelianos finitos multiplicativos das unidades do corpo finito $\mathbb{F}_p$ e o diagrama de Hasse de espaços projetivos $\mathbb{P}(\mathbb{F}_p^m)$. O uso dessa estrutura algébrica via o isomorfismo estabelecido visa fornecer elementos algébricos que possam ser úteis na construção de códigos de subespaços n-shot. O paralelo que pode ser traçado, para o caso binário, é que os vértices de um hipercubo é uma representação onde extraímos os códigos de bloco. O mesmo ocorre com o diagrama de Hasse. Note que os vértices de um hipercubo está associado a uma palavra-código. O mesmo ocorre com os "vértices"do diagrama de Hasse associado ao espaço projetivo como sendo um subespaço (palavra-código).

4.1 Relações entre Design Combinatório e Espaços Projetivos

Nesta seção, evidenciamos por meio de alguns exemplos, a relação entre design combinatório e espaços projetivos, ou seja, ilustramos a existência de uma estrutura combinatória associada aos espaços projetivos.

Teorema 4.1. *Seja $q \geq 2$ é uma potência de primo e $d \geq 2$ um inteiro. Então existe um design combinatório simétrico*

$$\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right) - BIBD.$$

Corolário 4.1. *Para cada potência de primo $q \geq 2$ e $d = 2$, existe um $(q^2+q+1, q+1, 1)$-BIBD simétrico, isto é, um plano projetivo de ordem q.*

As demonstrações do Teorema 4.1 e do Corolário 4.1 podem ser encontradas em (STINSON, 2004).

A seguir, apresentamos alguns exemplos que associam o design combinatório do Corolário 4.1 à uma classe de espaço projetivo $\mathbb{P}(\mathbb{F}_p^3)$, onde p é um primo.

Exemplo 4.1. *O design combinatório* $(7, 3, 1)$*-BIBD (plano projetivo de ordem 2) descreve as conexões entre os subespaços de dimensão 1 e dimensão 2 do espaço projetivo* $\mathbb{P}(\mathbb{F}_2^3)$*, ver Figura 11.*

Exemplo 4.2. *O design combinatório* $(13, 4, 1)$*-BIBD (plano projetivo de ordem 3) descreve as conexões entre os subespaços de dimensão 1 e dimensão 2 do espaço projetivo* $\mathbb{P}(\mathbb{F}_3^3)$*, ver Figura 15.*

Exemplo 4.3. *O design combinatório* $(p^2+p+1, p+1, 1)$*-BIBD simétrico (plano projetivo de ordem p primo) descreve as conexões entre os subespaços de dimensão 1 e dimensão 2 do espaço projetivo* $\mathbb{P}(\mathbb{F}_p^3)$*.*

4.2 Estrutura Algébrica de uma Classe de Espaços Projetivos

Nesta seção, apresentamos um isomorfismo entre uma classe de espaços projetivos $\mathbb{P}(\mathbb{F}_p^m)$ e uma estrutura algébrica, o grupo das unidades do corpo finito $\mathbb{F}_p$, por meio do diagrama de Hasse e do reticulado de grupo.

Considere um grupo multiplicativo C_p, onde p é um número primo, isto é, $C_p = (\{1, 2, 3, ..., p-1\}, \odot_p)$, com $\odot_p$ o produto representando módulo p. Neste contexto, e de acordo com o Exemplo 2.24 do Capítulo 2, é possivel construir o reticulado de grupo ou diagrama de Hasse, visto que C_p com a relação de inclusão é um conjunto parcialmente ordenado. Além disso,dois subgrupos estão conectados se, e somente se, G_1 é subgrupo de G_2 e a ordem $|G_1| = p.|G_2|$ ou vice-versa.

Exemplo 4.4. *Dados dois grupos finitos multiplicativos denotados por* $C_2 = \langle a \rangle = \{1, a\}$ *e* $C_2 = \langle b \rangle = \{1, b\}$*, então* $C_2 \times C_2 = \{1 = (1, 1), a = (a, 1), b = (1, b), ab = (a, b)\}$ *é um grupo com a operação* $*$ *definida*

$*$	1	ab	a	b
1	1	ab	a	b
ab	ab	1	b	a
a	a	b	1	ab
b	b	a	ab	1

Tabela 4 – Tabela de Cayley do Grupo $(C_2 \times C_2, *)$

Exemplo 4.5. *Dados três grupos finitos multiplicativos denotados por* $C_2 = \langle a \rangle = \{1, a\}$*,* $C_2 = \langle b \rangle = \{1, b\}$ *e* $C_2 = \langle c \rangle = \{1, c\}$*, então:*

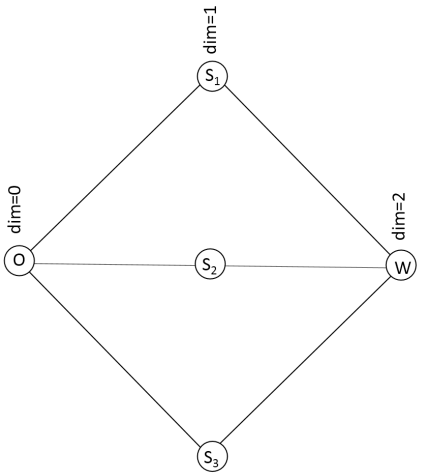
$$C_2 \times C_2 \times C_2 = \{1 = (1, 1, 1),\ a = (a, 1, 1),\ b = (1, b, 1),\ c = (1, 1, c),\ ab = (a, b, 1),\\ ac = (a, 1, c), bc = (1, b, c), abc = (a, b, c)\}$$

é um grupo com a operação $*$ *definida por*

$*$	1	abc	ab	bc	ac	a	b	c
1	1	abc	ab	bc	ac	a	b	c
abc	abc	1	c	a	b	bc	ac	ab
ab	ab	c	1	ac	bc	b	a	abc
bc	bc	a	ac	1	ab	abc	c	b
ac	ac	b	bc	ab	1	c	abc	a
a	a	bc	b	abc	c	1	ab	ac
b	b	ac	a	c	abc	ab	1	bc
c	c	ab	abc	b	a	ac	bc	1

Tabela 5 – Tabela de Cayley do Grupo $(C_2 \times C_2 \times C_2, *)$

Exemplo 4.6. *Seja o isomorfismo, via o correspondente diagrama de Hasse do espaço projetivo* $\mathbb{P}(\mathbb{F}_2^2)$ *e o reticulado do grupo* $G = C_2 \times C_2$ *de ordem 4, onde* $\times$ *denota o produto direto, como ilustrado nas Figura 9 e Figura 10.*



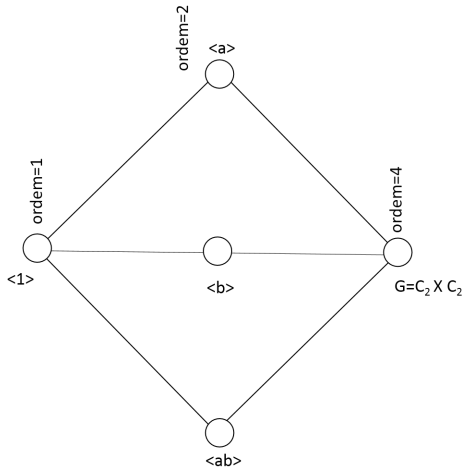


Figura 9 – Diagrama de Hasse do $\mathbb{P}(\mathbb{F}_2^2)$ Figura 10 – Reticulado do $G = C_2 \times C_2$

Onde os elementos do diagrama de Hasse associado ao espaço projetivo $\mathbb{P}(\mathbb{F}_2^2)$ *e o reticulado associado ao grupo* $G = C_2 \times C_2$ *são respectivamente,*

$$\mathbb{P}(\mathbb{F}_2^2) = \{O = \{00\},\ S_1 = \{00, 01\},\ S_2 = \{00, 10\},\ S_3 = \{00, 11\},\ W = \{00, 01, 10, 11\}\}$$

e

$$R(G = C_2 \times C_2) = \{\langle 1\rangle = (1,1),\ \langle a\rangle = \{(1,1),(a,1)\},\ \langle b\rangle = \{(1,1),(1,b)\},$$
$$\langle ab\rangle = \{(1,1),(a,b)\},\ G = \{(1,1),(a,1),(1,b),(a,b)\}\}.$$

Neste caso, apresentamos a seguinte aplicação φ

$$\varphi(x) = \begin{cases} \langle 1 \rangle, & se \quad x = O \\ \langle a \rangle, & se \quad x = S_1 \\ \langle b \rangle, & se \quad x = S_2 \\ \langle ab \rangle, & se \quad x = S_3 \\ G, & se \quad x = W \end{cases}$$

que claramente é um isomorfismo de conjuntos ordenados, $\varphi : \mathbb{P}(\mathbb{F}_2^2) \to G = C_2 \times C_2$.

Exemplo 4.7. *Via o isomorfismo no Exemplo 4.6, podemos associar o código do Exemplo 3.4 do Capítulo 3 ao código de grupo* $\{G_1 = \langle b \rangle = \{1, b\}, G_2 = \langle a \rangle = \{1, a\}\}$. *A partir desse isomorfismo podemos utilizar o código de subespaço n-shot para estender o código de grupo.*

Exemplo 4.8. *Novamente, seja o isomorfismo via o correspondente diagrama de Hasse do espaço projetivo* $\mathbb{P}(\mathbb{F}_2^3)$ *e o reticulado do grupo* $G = C_2 \times C_2 \times C_2$ *de ordem 8, como mostrado nas Figuras 11 e 12.*

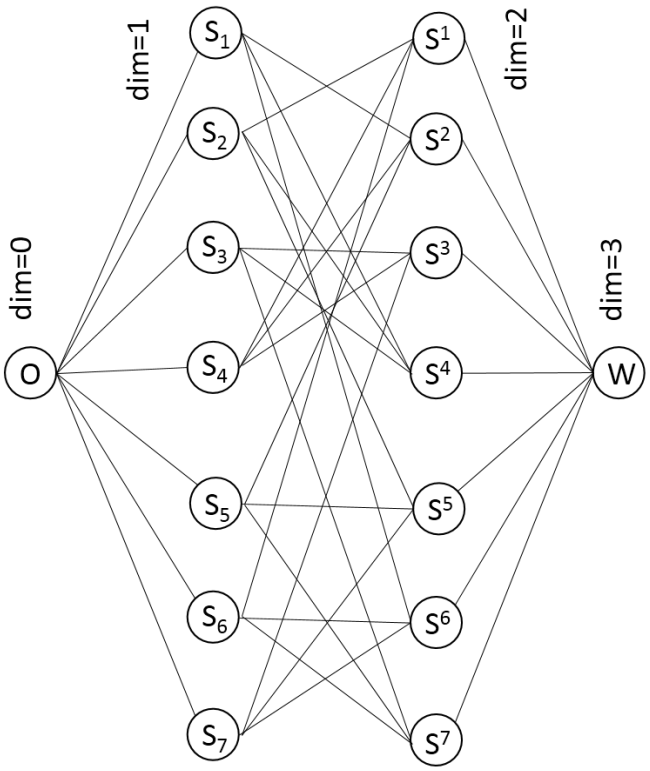


Figura 11 – Diagrama de Hasse do Espaço Projetivo $\mathbb{P}(\mathbb{F}_2^3)$

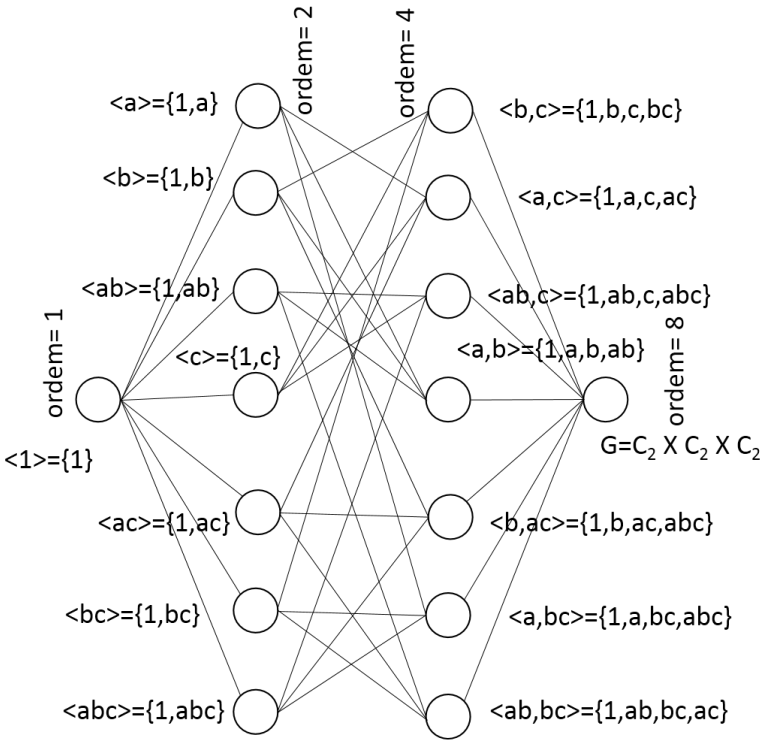


Figura 12 – Reticulado do Grupo $G = C_2 \times C_2 \times C_2$

Observe que podemos explicitar um isomorfismo associando os elementos do diagrama de Hasse, Figura 11, e os elementos do reticulado de grupo, Figura 12, definindo uma função φ que seja uma bijeção isótona com inversa isótona.

Exemplo 4.9. *Dado o isomorfismo no Exemplo 4.8, podemos associar o código do Exemplo 3.5 do Capítulo 3 ao código de grupo* $\mathcal{C} = \{G_1 = \langle a, b\rangle = \{1, a, b, ab\}, G_2 = \langle b, c\rangle = \{1, b, c, bc\}, G_3 = \langle a, c\rangle = \{1, a, c, ac\}\}$. *A partir desse isomorfismo podemos utilizar o código de subespaço n-shot para estender o código de grupo.*

Exemplo 4.10. *Seja o isomorfismo, via o correspondente diagrama de Hasse do espaço projetivo* $\mathbb{P}(\mathbb{F}_3^2)$ *e o reticulado do grupo* $G = C_3 \times C_3$ *de ordem 9.*

Neste caso, apresentamos a aplicação φ que associa os elementos do diagrama de Hasse Figura 13 e o reticulado de grupo Figura 14 e que claramente é um isomorfismo, ou seja, uma bijeção isótona com inversa isótona, $\varphi : \mathbb{P}(\mathbb{F}_3^2) \to G = C_3 \times C_3$ definida por:

$$\varphi(x) = \begin{cases} \langle 1\rangle, & se \;\; x = O \\ \langle a, b\rangle, & se \;\; x = S_1 \\ \langle c, d\rangle, & se \;\; x = S_2 \\ \langle ac, bd\rangle, & se \;\; x = S_3 \\ \langle ad, bc\rangle, & se \;\; x = S_4 \\ G, & se \;\; x = W \end{cases}$$

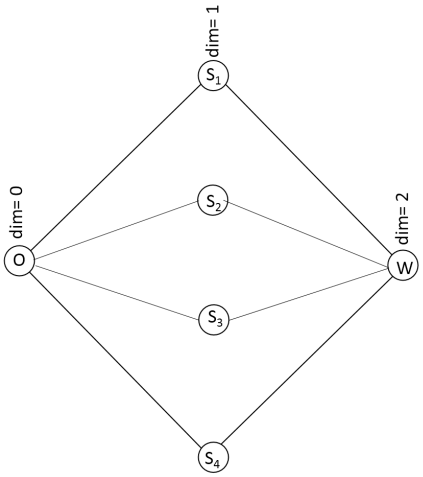


Figura 13 – Diagrama do $\mathbb{P}(\mathbb{F}_3^2)$

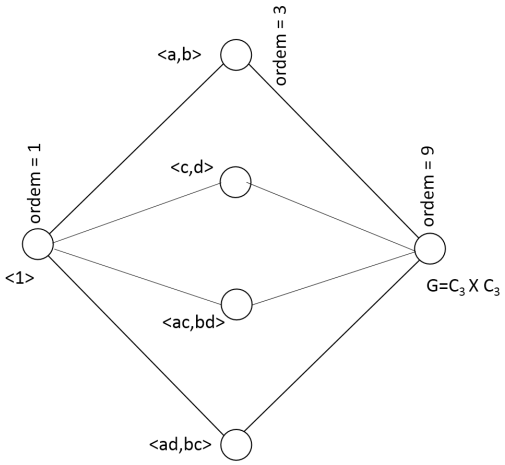


Figura 14 – Reticulado do $G = C_3 \times C_3$

Exemplo 4.11. *Seja o isomorfismo, via o correspondente diagrama de Hasse do espaço projetivo* $\mathbb{P}(\mathbb{F}_3^3)$ *e o reticulado do grupo* $G = C_3 \times C_3 \times C_3$ *de ordem 27, por meio do design combinatório* $(13, 4, 1)$*-BIBD.*

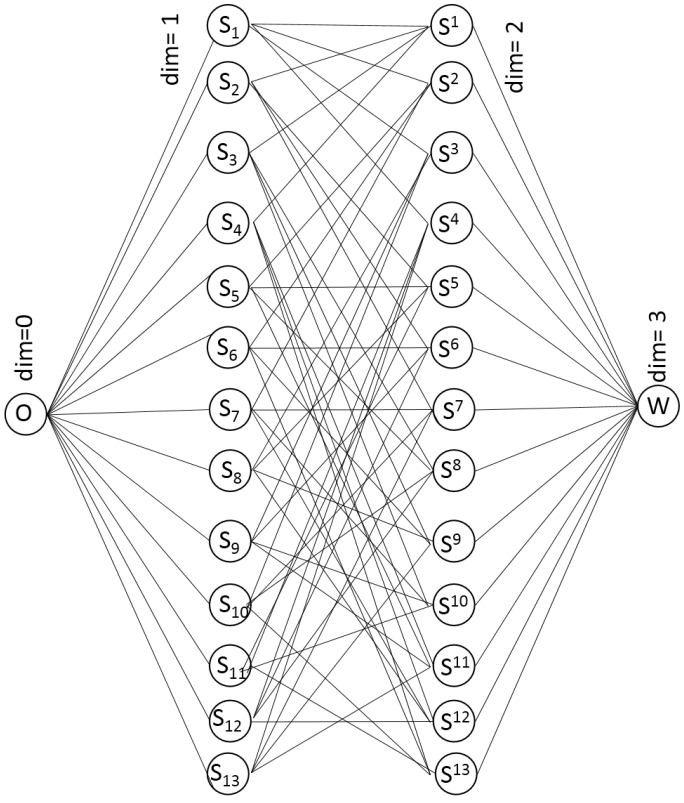


Figura 15 – Diagrama de Hasse do Espaço Projetivo $\mathbb{P}(\mathbb{F}_3^3)$

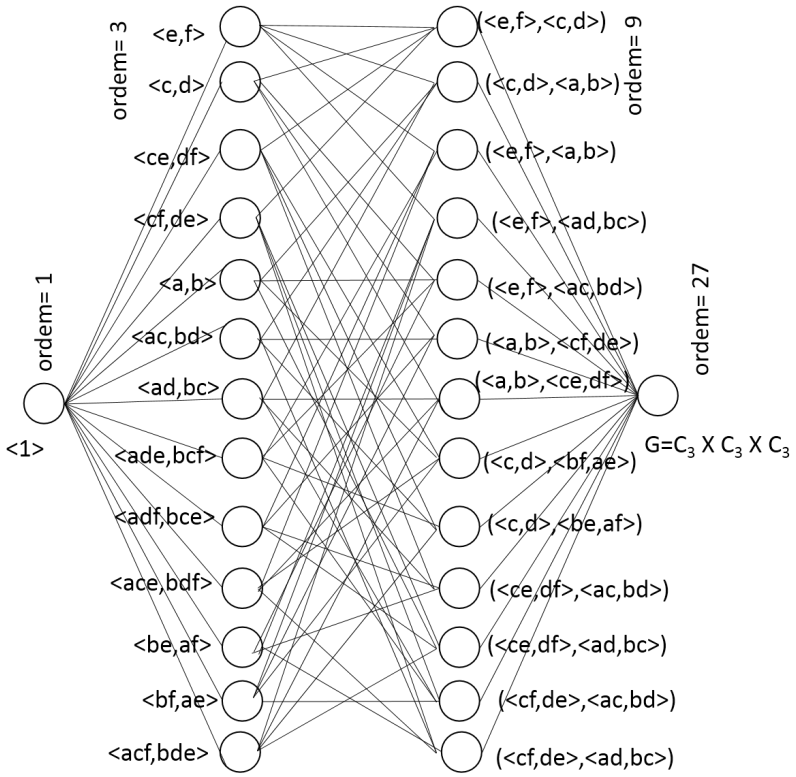


Figura 16 – Reticulado do Grupo $G = C_3 \times C_3 \times C_3$

Observe que podemos explicitar um isomorfismo associando os elementos do diagrama de Hasse, Figura 15, e os elementos do reticulado de grupo, Figura 16, definindo uma função φ que seja uma bijeção isótona com inversa isótona. Podemos generalizar os exemplos anteriores observando que dado o design combinatório $(p^2+p+1, p+1, 1)$-BIBD simétrico, com p -primo, que descreve o espaço projetivo $\mathbb{P}(\mathbb{F}_p^3)$ e dada a estrutura algébrica $G = C_p \times C_p \times C_p$ de ordem p^3, que possui subgrupos de ordem p^2, ordem p e ordem 1. Podemos construir um isomorfismo entre o diagrama de Hasse associado ao espaço projetivo $\mathbb{P}(\mathbb{F}_q^3)$ e o reticulado de grupo associado ao grupo $G = C_p \times C_p \times C_p$ que descreve a mesma estrutura combinatória. O número de subgrupos de ordem p^2 é dado por:

$$\binom{3}{2}_p = \prod_{i=0}^{k-1} \frac{p^3 - p^i}{p^2 - p^i} = \frac{p^3-1}{p^2-1}\frac{p^3-p}{p^2-p} = p^2 + p + 1.$$

E a quantidade de subgrupos de ordem p é dado por:

$$\binom{3}{1}_p = \prod_{i=0}^{k-1} \frac{p^3 - p^i}{p - p^i} = \frac{p^3-1}{p-1} = p^2 + p + 1.$$

Note que para $p = 2$ o número de subgrupos de ordens 2 e 4 é igual a 7, ver Exemplo 4.8. Para $p = 3$, o número de subgrupos cujas ordens são 3 e 9 é igual a 13, ver

Exemplo 4.11.

Tais observações são caracterizadas através da seguinte proposição.

Proposição 4.1. *Seja a estrutura algébrica $G = C_p \times C_p \times \cdots \times C_p$ de ordem p^m. O diagrama de Hasse associado ao espaço projetivo $\mathbb{P}(\mathbb{F}_p^m)$ e o reticulado de grupo associado ao grupo $G = C_p \times C_p \times \cdots \times C_p$, são isomorfos.*

Observação 4.1. *Como $\mathbb{F}_p^m \approx \mathbb{F}_{p^m}$, segue que o diagrama de Hasse associado ao espaço projetivo $\mathbb{P}(\mathbb{F}_p^m)$ é isomorfo ao reticulado de grupo associado ao grupo $(C_p)^m$, onde C_p é o grupo das unidades do corpo $\mathbb{F}_p$.*

A seguir, apresentamos um exemplo quando fixamos $p = 2$. Associando ao espaço projetivo $\mathbb{P}(\mathbb{F}_2^m)$ obtemos uma estrutura algébrica $G = C_2 \times C_2 \times C_2 \times ... \times C_2$ de ordem 2^m, cujos subgrupos possuem ordens $1, 2^1, 2^2, ..., 2^m$ e decorre que esta estrutura algébrica descreve a mesma estrutura combinatória que o espaço projetivo $\mathbb{P}(\mathbb{F}_2^m)$.

Exemplo 4.12. *Existe um isomorfismo entre o diagrama de Hasse do espaço projetivo $\mathbb{P}(\mathbb{F}_2^4)$ e o reticulado do grupo $G = C_2 \times C_2 \times C_2 \times C_2$ de ordem 16, evidenciado por meio do design combinatório $(15, 3, 1)$-BIBD. O espaço projetivo $\mathbb{P}(\mathbb{F}_2^4)$ possui 1 subespaço de dimensão 0, 15 subespaço de dimensão 1, 35 subespaços de dimensão 2, 15 subespaços de dimensão 3 e 1 subespaço de dimensão 4, conforme os cálculos a seguir:*

$$\binom{4}{4}_2 = \binom{4}{0}_2 = 1.$$

$$\binom{4}{3}_2 = \binom{4}{1}_2 = \frac{2^3 - 2^0}{2^1 - 2^0} = \frac{2^4 - 1}{2 - 1} = 15.$$

$$\binom{4}{2}_2 = \prod_{i=0}^{1} \frac{2^4 - 2^i}{2^2 - 2^i} = \frac{2^4 - 2^0}{2^2 - 2^0} \cdot \frac{2^4 - 2^1}{2^2 - 2^1} = \frac{16 - 1}{4 - 1} \cdot \frac{16 - 2}{4 - 2} = 5.7 = 35.$$

O design combinatório $(15, 3, 1)$-BIBD é caracterizado através dos conjuntos

$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$$

e

$$\begin{array}{ccccccc} B = \{(1,2,3), & (1,4,5), & (1,6,7), & (1,8,9), & (1,10,11), & (1,12,13), & (1,14,15), \\ (2,14,15), & (3,4,7), & (2,5,7), & (3,5,6), & (2,8,9), & (3,8,11), & (2,9,11), \\ (3,9,10), & (2,12,14), & (3,12,15), & (2,13,15), & (3,13,14), & (4,8,12), & (5,8,13), \\ (4,9,13), & (5,9,12), & (6,8,14), & (7,8,15), & (6,9,15), & (7,9,14), & (4,10,14), \\ (5,10,15), & (4,11,15), & (5,11,14), & (6,10,12), & (7,10,13), & (6,11,13), & (7,11,12)\} \end{array}$$

e descreve as conexões entre os subespaços de dimensões 1 e 2. Observe que está destacado em "vermelho"o bloco $(1,2,3)$*, no diagrama de Hasse do espaço projetivo* $\mathbb{P}(\mathbb{F}_2^4)$*, ver Figura 17. De modo análogo, as conexões entre os subespaços de dimensões 2 e 3, são descritas pelo design combinatório e dado por*

$$X = \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$$

e

$$\begin{array}{ccccccc} B = \{(1,2,3), & (1,4,6), & (1,5,7), & (2,4,5), & (2,6,7), & (3,4,7), & (3,5,6), \\ (1,8,12), & (1,9,13), & (1,10,14), & (1,11,15), & (2,8,10), & (2,9,11), & (2,12,14), \\ (2,13,15), & (3,8,14), & (3,9,15), & (3,10,12), & (3,11,13), & (4,8,9), & (4,10,11), \\ (4,12,13), & (4,14,15), & (5,8,11), & (5,9,10), & (5,12,15), & (5,13,14), & (6,8,13), \\ (6,10,15), & (6,9,12), & (6,11,14), & (7,8,15), & (7,10,13), & (7,11,12), & (7,9,14)\}, \end{array}$$

e está destacado em "azul"o bloco $(1,9,13)$ *na Figura 17. O grupo* G *apresenta subgrupos de ordem 1,2,4,8 e 16.*

Ordem 1:

$$\langle 1\rangle = \{1\}$$

Ordem 2:

$$\begin{array}{c} \langle a\rangle = \{1,a\}, \langle b\rangle = \{1,b\}, \langle c\rangle = \{1,c\}, \langle d\rangle = \{1,d\}, \\ \langle ab\rangle = \{1,ab\}, \langle ac\rangle = \{1,ac\}, \langle ad\rangle = \{1,ad\}, \langle bc\rangle = \{1,bc\}, \\ \langle bd\rangle = \{1,a\}, \langle cd\rangle = \{1,cd\}, \langle abc\rangle = \{1,abc\}, \langle abd\rangle = \{1,abd\}, \\ \langle acd\rangle = \{1,acd\}, \langle bcd\rangle = \{1,bcd\}, \langle abcd\rangle = \{1,abcd\}. \end{array}$$

Ordem 4:

$$\langle a,b\rangle = \{1,a,b,ab\}, \langle a,c\rangle = \{1,a,c,ac\}, \langle a,d\rangle = \{1,a,d,ad\},$$
$$\langle b,c\rangle = \{1,b,c,bc\}, \langle b,d\rangle = \{1,b,d,bd\}, \langle c,d\rangle = \{1,c,d,cd\},$$
$$\langle a,bc\rangle = \{1,a,bc,abc\}, \langle a,bd\rangle = \{1,a,bd,abd\}, \langle a,cd\rangle = \{1,a,cd,acd\},$$
$$\langle b,ac\rangle = \{1,b,ac,abc\}, \langle b,ad\rangle = \{1,b,ad,abd\}, \langle c,ab\rangle = \{1,c,ab,abc\},$$
$$\langle c,ad\rangle = \{1,c,ad,acd\}, \langle c,bd\rangle = \{1,c,bd,bcd\}, \langle d,ab\rangle = \{1,d,ab,abd\},$$
$$\langle d,ac\rangle = \{1,d,ac,acd\}, \langle d,bc\rangle = \{1,d,bc,bcd\}, \langle a,bcd\rangle = \{1,a,bcd,abcd\},$$
$$\langle b,acd\rangle = \{1,b,acd,abcd\}, \langle c,abd\rangle = \{1,c,abd,abcd\}, \langle d,abc\rangle = \{1,d,abc,abcd\},$$
$$\langle ab,ac\rangle = \{1,ab,ac,bc\}, \langle ab,ad\rangle = \{1,ab,ad,bd\}, \langle ab,cd\rangle = \{1,ab,cd,abcd\},$$
$$\langle ac,ad\rangle = \{1,ac,ad,cd\}, \langle ac,bd\rangle = \{1,ac,bd,abcd\}, \langle ad,bc\rangle = \{1,ad,bc,abcd\},$$
$$\langle bc,bd\rangle = \{1,bc,bd,cd\}, \langle abc,abd\rangle = \{1,abc,abd,cd\}, \langle abc,acd\rangle = \{1,abc,acd,bd\},$$
$$\langle abc,bcd\rangle = \{1,abc,bcd,ad\}, \langle abd,acd\rangle = \{1,abd,acd,bc\},$$
$$\langle abd,bcd\rangle = \{1,abd,bcd,ac\}, \langle acd,bcd\rangle = \{1,acd,bcd,ab\}.$$

Ordem 8:

$$\langle a,b,c\rangle = \{1,a,b,c,ab,ac,bc,abc\}, \langle a,b,d\rangle = \{1,a,b,d,ab,ad,bd,abd\},$$
$$\langle a,c,d\rangle = \{1,a,c,d,ac,ad,cd,acd\}, \langle ab,ac,bd\rangle = \{1,ab,ac,bd,bc,ad,cd,abcd\},$$
$$\langle a,bc,bd\rangle = \{1,a,bc,bd,cd,abc,abd,acd\}, \langle b,ac,ad\rangle = \{1,b,ac,ad,cd,abc,abd,bcd\},$$
$$\langle d,ab,ac\rangle = \{1,d,ab,ac,bc,abd,acd,bcd\}, \langle c,ad,bd\rangle = \{1,c,ad,bd,ab,acd,bcd,abc\},$$
$$\langle c,d,ab\rangle = \{1,c,d,ab,cd,abc,abd,abcd\}, \langle a,b,cd\rangle = \{1,a,b,cd,ab,acd,bcd,abcd\},$$
$$\langle a,c,bd\rangle = \{1,a,c,bd,ac,abd,bcd,abcd\}, \langle a,d,bc\rangle = \{1,a,d,bc,ad,abc,bcd,abcd\},$$
$$\langle b,c,ad\rangle = \{1,b,c,ad,bc,abd,acd,abcd\}, \langle b,d,ac\rangle = \{1,b,d,ac,bd,abc,acd,abcd\}.$$

Ordem 16:

$$G = \langle a,b,c,d\rangle = \{1,a,b,c,d,ab,ac,ad,bc,bd,cd,abc,abd,acd,bcd,abcd\}.$$

Observe que temos 15 subgrupos de ordem 2, 35 subrupos de ordem 4 e 15 subgrupos de ordem 8. Cada subgrupo de ordem 2 é subgrupo de 7 subgrupos de ordem 4. Assim como cada subgrupo de ordem 8 é subgrupo de 3 subgrupos de ordem 8. A menos de permutação dos elementos dos grupos de ordem 2 ou dos subespaços de dimensão 2, o diagrama de Hasse (ver Figura 17) do espaço projetivo $\mathbb{P}(\mathbb{F}_2^4)$ e o reticulado do grupo (ver Figura 18) $G = C_2 \times C_2 \times C_2 \times C_2$ são isomorfos.

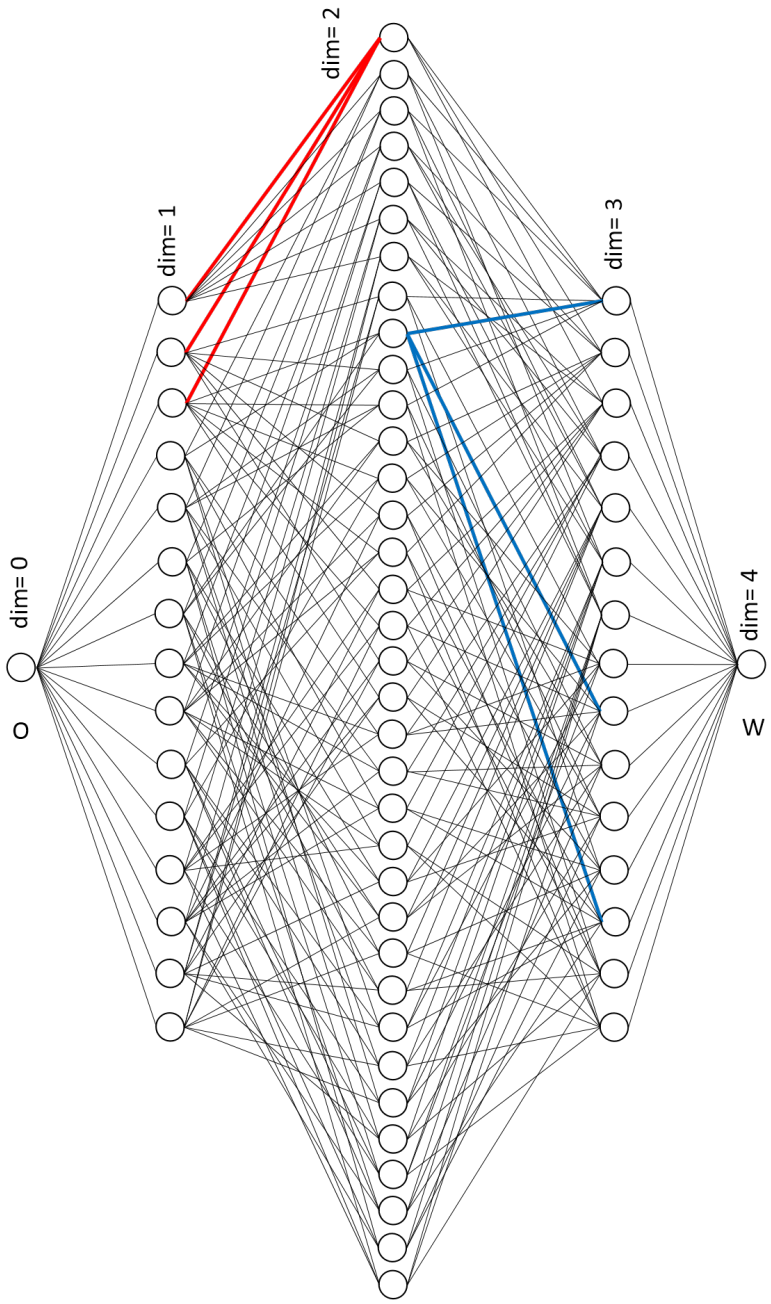


Figura 17 – Diagrama de Hasse do Espaço Projetivo $\mathbb{P}(\mathbb{F}_2^4)$

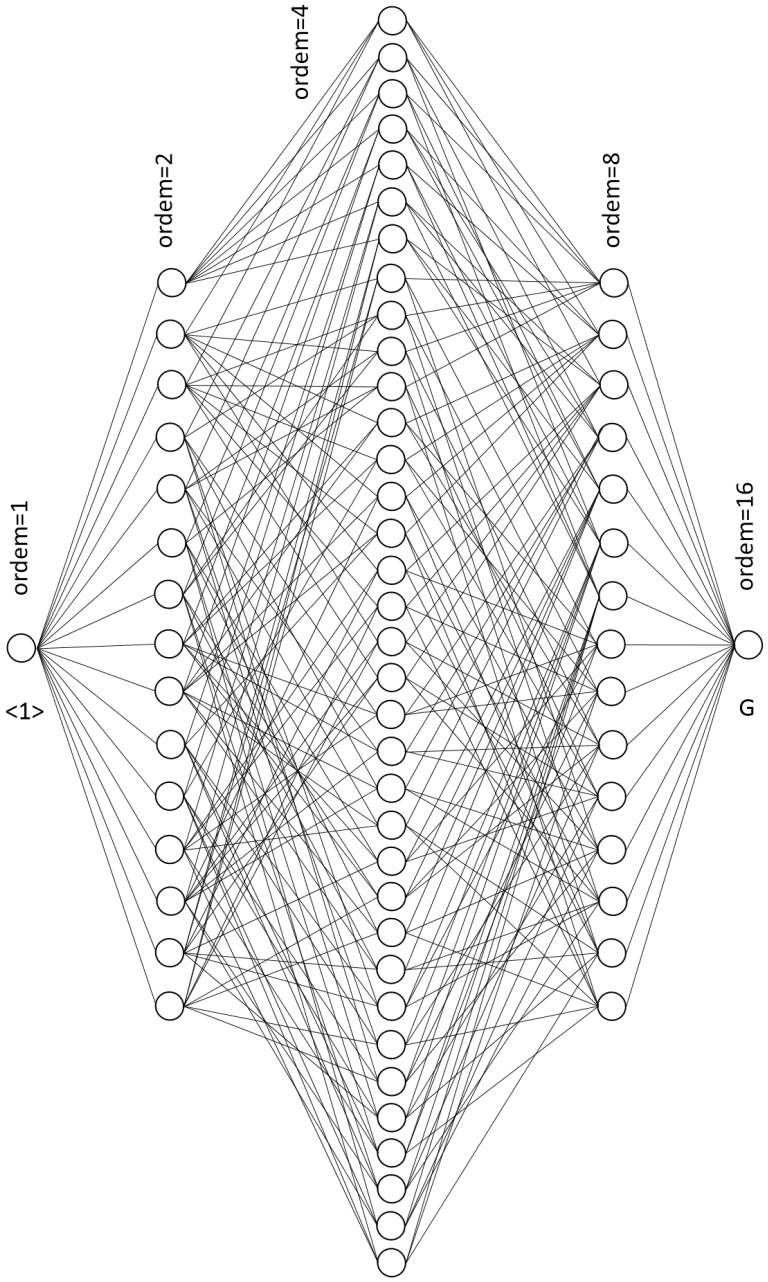


Figura 18 – Reticulado do Grupo $G = C_2 \times C_2 \times C_2 \times C_2$

Corolário 4.2. *O diagrama de Hasse associado ao espaço projetivo* $\mathbb{P}(\mathbb{F}_2^m)$ *e o reticulado do grupo* $G = C_2 \times C_2 \times C_2 \times ... \times C_2$ *de ordem* 2^m*, são isomorfos.*

5 Códigos Quânticos de Subespaços na grassmanniana

O trabalho de (IMAI; HIRAKAWA, 1977) impulsionou a forma de projetar códigos para canais gaussianos e canais contínuos de uma forma mais geral. Nessa proposta as operações de modulação e codificação são realizadas simultaneamente, num processo de codificação multinível fazendo uso de vários códigos de blocos binários. Esta técnica é conhecida como modulação codificada. A técnica de modulação codificada consolidou-se de vez com o trabalho de (UNGERBOEK, 1982) consistindo na implementação de sistemas de comunicações digitais onde as operações de modulação e codificação são realizadas simultaneamente, de modo que ganhos significativos de codificação poderiam ser obtidos, sem a necessidade de diminuir a taxa de transmissão de informação nem a expansão da faixa. Este método é denominado ***mapeamento por particionamento de conjuntos***, e consiste em particionar sucessivamente o conjunto de pontos do espaço de sinais em subconjuntos com uma distância euclidiana mínima progressivamente crescente.

Neste capítulo, nossa proposta é utilizar a ideia do mapeamento por particionamento de conjuntos para relacionar códigos de subespaços à estado quântico puro separável universal e estado quântico de máximo emaranhamento global, dando origem aos códigos quânticos de subespaços. O estudo do emaranhamento quântico é fundamental para aplicações em informação quântica e computação quântica, tais como a codificação superdensa, o teletransporte e a criptografia quântica.

O trabalho de doutorado de (GAZZONI, 2008) propõe que o conjunto de sequências binárias que constituem os kets de um estado quântico puro arbitrário de máximo emaranhamento global possa ser descrito por códigos binários lineares com a máxima distância de Hamming e alguns códigos binários não lineares, através da medida de Meyer-Wallach. A partir desta interpretação é possível descrever estado quântico puro arbitrário de máximo emaranhamento global e estudar, tendo como base elementos de teoria da codificação, quais dentre todos os possíveis estados são mais apropriados para serem empregados em tarefas de processamento de informação quântica. Tal resultado foi verificado a partir da identificação entre as representações dos kets de um estado quântico puro arbitrário com n *q-bits* e os vértices de um n-cubo unitário.

Considerando a n-esfera que circunscreve este cubo, temos que o problema de descrever as combinações de kets que compõem um estado quântico arbitrário é equivalente ao problema de descrever conjuntos de pontos na superfície desta esfera. Sob esta interpretação, determinar as configurações de um estado puro de máximo emaranhamento global é equivalente a determinar códigos de Slepian (SLEPIAN, 1968) sob a condição de

que o canal é Gaussiano aditivo, sem restrição de faixa e com símbolos equiprováveis na entrada do canal.

Como já dito nosso objetivo é utilizar as técnicas de modulação codificada para podermos rotular códigos de subespaços específicos e associarmos ao estado quântico puro separável ou emaranhado (MACWILLIAMS; SLOANE, 1983; GAZZONI, 2008). Podemos reinterpretar o problema em questão, e identificar o conjunto de sequências binárias que constituem os kets de um estado quântico puro arbitrário de máximo emaranhamento global à códigos de subespaços, sendo assim, podemos representar um estado quântico puro arbitrário com n *q-bits* por meio de um código de subespaço específico do espaço projetivo $\mathbb{P}(\mathbb{F}_2^m)$. Assim, podemos também utilizar a teoria de códigos de subespaços n-shot para estabelecer novos estados quânticos de máximo emaranhamento global, verificado por meio da medida de Meyer-Wallach.

Este capítulo está organizado da seguinte forma. Na Seção 5.1, apresentamos os postulados da mecânica quântica que fundamentam os estudos e pesquisas em computação quântica e informação quântica. Na Seção 5.2, apresentamos as principais definições e resultados sobre estados quânticos puros arbitrários. Na seção 5.3 são estabelecidas as principais definições e resultados sobre mapeamento por particionamento de conjuntos. Na Seção 5.4, são fornecidas algumas definições e exemplos de rotulamento de códigos de órbita de subespaços associado a estado quântico puro separável universal, bem como, usamos os códigos de subespaços n-shot para obter novos estados quânticos de máximo emaranhamento global. Na Seção 5.5, apresentamos exemplos de rotulamento de códigos de órbita de subespaço associado diretamente ao estado quântico de máximo emaranhamento global.

5.1 Fundamentos de Computação Quântica e Informação Quântica

Nesta seção, faremos uma revisão de conceitos da mecânica quântica necessários ao entendimento da proposta considerada.

5.1.1 Postulados da Mecânica Quântica

Mecânica quântica é a parte da física responsável pelo estudo do comportamento de átomos, elétrons, moléculas, entre outras, cujos postulados foram desenvolvidos através de um longo processo. Em essência, consideramos a mecânica quântica como sendo uma estrutura matemática que permite descrever sistemas quânticos (NIELSEN; CHUANG, 2000; LIMA, 2007).

Postulado 1: Existe um espaço vetorial complexo, com produto interno, associado a qualquer sistema físico *fechado* (sistema que não interage com outros sistemas). Um

estado desse sistema é completamente descrito por um vetor unitário, chamado **vetor de estado**.

A unidade de informação quântica ou sistema quântico que nos interessa é o **bit quântico** ou *q-bit*, cujo espaço vetorial associado é o $\mathbb{C}^2$, com o produto interno usual. Uma base ortonormal para esse espaço pode ser dada pelos vetores $|0\rangle$ e $|1\rangle$, que serão representados usando a **notação de Dirac**:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

e

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

A representação matemática de um *q-bit* é um vetor unitário de $\mathbb{C}^2$. Um estado arbitrário $|\psi\rangle$ nesse sistema pode ser descrito por

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

onde $\alpha, \beta \in \mathbb{C}$ e a restrição $|\alpha|^2 + |\beta|^2 = 1$ deve ser satisfeita. A base $\{|0\rangle, |1\rangle\}$ é chamada **base computacional** e o vetor $|\psi\rangle$ denota a **superposição** dos vetores $|0\rangle$ e $|1\rangle$, com **amplitudes** α e β (usaremos os termos vetor e estado indistintamente).

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

$$|\psi_2\rangle = U|\psi_1\rangle.$$

Apresentamos alguns conceitos importantes para compreensão dos próximos postulados: **dual, produto interno** e **produto externo**. O dual de um vetor $|\varphi\rangle \in \mathbb{C}^n$, denotado por $\langle\varphi|$, é o vetor transposto de $|\varphi\rangle$ com os elementos substituídos pelos seus correspondentes complexos conjugados, ou seja,

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

Matricialmente, no caso de um *q-bit*, dado por

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

temos que o dual de $|\varphi\rangle$ é

$$\langle\varphi| = \left(\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \right)^\dagger = [\alpha^* \ \beta^*].$$

Dados dois vetores $|\varphi\rangle, |\psi\rangle \in \mathbb{C}^n$, o produto interno $\langle\varphi|\psi\rangle$ e o produto externo $|\varphi\rangle\langle\psi|$ são definidos, respectivamente, por

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

e

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

Note que $|\varphi\rangle, |\psi\rangle$ são vetores "coluna " e $\langle\varphi|, \langle\psi|$ são vetores "linha".

Exemplo 5.1. *Considerando os vetores da base computacional, o produto interno e externo são dados, respectivamente, por*

$$\langle 0|1\rangle = [1\ 0]\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1.0 + 0.1 = 0$$

e

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

A interpretação física do *q-bit* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, para α e β não nulos, é que ele está simultaneamente nos estados $|0\rangle$ e $|1\rangle$. Para tornar a informação acessível ao nível clássico, precisamos aplicar uma medida. Para considerar esse fato, existe um terceiro postulado.

Postulado 3: As medidas sobre sistemas quânticos são descritas por operadores **hermitianos** M ($M^\dagger = M$), chamados **observáveis**. Pelo fato de M ser hermitiano, podemos escrever

$$M = \sum_{i=1}^{n} \lambda_i |i\rangle\langle i|,$$

onde $\{|i\rangle\}$, $i = 1, \cdots, n$, é uma base ortonormal de autovetores de M com os respectivos autovalores λ_i. Os possíveis resultados da medida correspondem aos autovalores λ_i de M. Supondo que o resultado da medida seja "λ_i", o estado $|\psi_{\lambda_i}\rangle$, após a medida, é dado por

$$|\psi_{\lambda_i}\rangle = \frac{(|i\rangle\langle i|)|\psi\rangle}{\sqrt{p_{\lambda_i}}}, \tag{5.1}$$

onde $|\psi\rangle$ é o estado anterior à medida e p_{λ_i} é a probalidade de se obter "λ_i", dada por

$$p_{\lambda_i} = \langle\psi|(|i\rangle\langle i|)|\psi\rangle. \tag{5.2}$$

Neste caso, a medida descrita no Postulado 3, chamada **medida projetiva**, é um caso particular de uma medida mais geral.

Em geral, o estado $|\psi\rangle$ com n *q-bits*, é uma superposição dos 2^n estados $|00\cdots.0\rangle + |00\cdots1\rangle + \cdots + |11\cdots1\rangle$, onde a sequência dentro de cada *ket* é a representação n-ária

dos números $0, 1, \cdots, 2^n - 1$ e é escrito como:

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle,$$

onde $\alpha_i \in \mathbb{C}, \quad \forall i \in \{0, 1, \cdots, 2^n - 1\}$ e com a restrição

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1.$$

Cabe observar que o princípio da superposição quando aplicado a sistemas compostos, ou seja, com mais de um *q-bit* implica em um fenômeno chamado **emaranhamento**.

Para caracterizar estados com mais de um *q-bit*, temos o seguinte postulado.

Postulado 4: O estado composto por n estados, $|\psi_1\rangle, |\psi_2\rangle, \cdots, |\psi_n\rangle$, é o produto tensorial $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

O produto tensorial $A \otimes B$, entre as matrizes $A \in \mathbb{C}^{m\times n}$ e $B \in \mathbb{C}^{p\times q}$ é definido como sendo a matriz

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix},$$

onde A_{ij} é o elemento da linha i e da coluna j de A. Note que a dimensão da matriz $A \otimes B$ é $mp \times nq$ e que o produto tensorial não é comutativo. Por exemplo,

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

e

$$|1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Usaremos também a notação $|v\rangle|w\rangle$ ou $|vw\rangle$ para o produto tensorial $|v\rangle \otimes |w\rangle$.

5.2 Estados Quânticos Puros Arbitrários e Principais Resultados

Nesta seção, faremos uma breve exposição das principais definições e resultados relativo ao estudo de estados quânticos puros arbitrários, para maiores detalhes e demonstração dos teoremas e proposições, consultar (GAZZONI, 2008).

Definição 5.1. *Um estado puro arbitrário com n q-bits* $|\psi\rangle_n$ *representado por*

$$|\psi\rangle_n = \alpha_0|000\cdots0\rangle + \alpha_1|000\cdots1\rangle + \cdots + \alpha_{2^n-1}|111\cdots1\rangle,$$

com $\alpha_0, \alpha_1, \cdots, \alpha_{2^n-1} \in \mathbb{C}$ *e* $\sum_{s=0}^{2^n-1} |\alpha_s|^2 = 1$ *é dito* ***estado separável*** *se puder ser escrito como* $|\psi\rangle_n = |\varphi_1\rangle_1 \otimes |\varphi_2\rangle_1 \otimes \cdots \otimes |\varphi_n\rangle_1$ *onde* $|\varphi_1\rangle_1, |\varphi_2\rangle_1, \cdots, |\varphi_n\rangle_1$ *são estados puros com 1 q-bit.*

Observação 5.1. *Qualquer estado que não admitir exatamente esta decomposição é considerado um* ***estado emaranhado****.*

Teorema 5.1. *Um critério de separabilidade para estados puros arbitrários com n q-bits como* $|\psi\rangle_n$*, é dado pelo conjunto de equações* $\alpha_i\alpha_j = \alpha_k\alpha_l$*, onde i,j,k e* $l \in \{0, 1, 2, \cdots, 2^n - 1\}$ *são escolhidos de acordo com as seguintes condições* $d_H(i, j) = d_H(k, l) = t$ *satisfazendo* $d_H(i, k) = d_H(j, l) = 1$ *e* $d_H(i, l) = d_H(j, k) = t - 1$ *onde* $2 \leq t \leq n$ *sendo* i, j, k, l *sequências binárias de comprimento n associadas, respectivamente, as amplitudes* $\alpha_i, \alpha_j, \alpha_k, \alpha_l$*, nesta ordem.*

Apresentamos, a seguir, a definição da medida de emaranhamento global para estados quânticos puros dada por Meyer-Wallach.

Definição 5.2. *Seja* $\boldsymbol{x}= x_1 \cdots x_n$ *uma n-upla binária associada ao conteúdo de um ket de* $|\psi\rangle_n$*, sendo* x_j*,* $j = 1, \cdots, n$*, cada coordenada de* $\boldsymbol{x}$*. Considere* $\iota_j(b) : (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n-1}$ *a aplicação linear definida pela seguinte ação na base:*

$$\iota_j(b)(|x_1\rangle \otimes \cdots \otimes |x_n\rangle) = \delta_{bx_j}|x_1\rangle \otimes \cdots \otimes |x_{j-1}\rangle \otimes |x_{j+1}\rangle \otimes \cdots |x_n\rangle,$$

onde $x_i \in \{0, 1\}$ *e* $b_i \in \{0, 1\}$*. Dado um estado quântico puro com n q-bits* $|\psi\rangle_n$*, a* ***medida de emaranhamento global de Meyer-Wallach*** *é dada por:*

$$Q(|\psi\rangle_n) = \frac{4}{n}\sum_{j=1}^{n} D(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle),$$

onde $D(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle) = \langle\psi|\iota_j(0), \iota_j(0)|\psi\rangle\langle\psi|\iota_j(1), \iota_j(1)|\psi\rangle - |\langle\psi|\iota_j(0), \iota_j(1)|\psi\rangle|^2$*, para todo* $j \in \{1, 2, \cdots, n\}$*.*

Observação 5.2. *Q é invariante sob transformações unitárias locais e tal que* $0 \leq Q \leq 1$*. Assim,* $Q(|\psi\rangle_n) = 0$ *se, e somente se,* $|\psi\rangle_n$ *é um estado separável, e* $Q(|\psi\rangle) = 1$ *se, e somente se,* $|\psi\rangle_n$ *é um estado puro de máximo emaranhamento global.*

Exemplo 5.2. *O estado* $|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$*.* $|\psi_{HGHZ}\rangle$ *pertence a uma classe de estados com três q-bits de máximo emaranhamento global obtida pela ação do operador de Hadamard (operador unitário) sobre cada um dos q-bits do estado GHZ (Greenberger-Horne-Zeilinger), (GREENBERGER D. M.; ZEILINGER, 1990). O*

objetivo é mostrar que $|\psi_{HGHZ}\rangle$ *é um estado de máximo emaranhamento global. De fato: observe que:*

$$\iota_1(0)|\psi_{HGHZ}\rangle = \iota_2(0)|\psi_{HGHZ}\rangle = \iota_3(0)|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}(|00\rangle + |11\rangle),$$

$$\iota_1(1)|\psi_{HGHZ}\rangle = \iota_2(1)|\psi_{HGHZ}\rangle = \iota_3(1)|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}(|10\rangle + |01\rangle).$$

Assim,

$$\begin{aligned} D &= (\tfrac{1}{\sqrt{4}})^2\langle(|00\rangle + |11\rangle)|(|00\rangle + |11\rangle)\rangle(\tfrac{1}{\sqrt{4}})^2\langle(|10\rangle + |01\rangle)|(|10\rangle + |01\rangle)\rangle + \\ &-(\tfrac{1}{\sqrt{4}})^2|\langle(|00\rangle + |11\rangle)|(|10\rangle + |01\rangle)\rangle|^2 \\ &= (\tfrac{1}{\sqrt{4}})^4[\langle 00|00\rangle + \langle 00|11\rangle + \langle 11|00\rangle + \langle 11|11\rangle][\langle 10|10\rangle + \langle 10|01\rangle + \langle 01|10\rangle + \langle 01|01\rangle] + \\ &-\tfrac{1}{\sqrt{4}})^2|(\langle 00|10\rangle + \langle 00|01\rangle + \langle 11|10\rangle + \langle 11|01\rangle)|^2 \\ &= 4(\tfrac{1}{\sqrt{4}})^4 = 4.(\tfrac{1}{4})^2 = \tfrac{1}{4},\ \textit{para } j = 1, 2, 3. \end{aligned}$$

Logo,

$$Q(|\psi_{HGHZ}\rangle) = \frac{4}{3}\sum_{j=1}^{3}\frac{1}{4} = 1.$$

Portanto, $|\psi_{HGHZ}\rangle$ *é um estado de máximo emaranhamento global.*

Proposição 5.1. *Seja* $|\psi\rangle$ *um estado quântico puro com amplitudes iguais a* $\frac{1}{\sqrt{M}}$ *e tal que o conjunto* A_ψ *(conjunto formado pelas sequências que caracteriza o estado quântico puro - código) satisfaz* $d > 1$*. Nestas condições, a seguinte equivalência é estabelecida:*

$$Q(|\psi\rangle) \equiv Q'(|\psi\rangle) = \frac{4}{n}.\frac{1}{M^2}\sum_{j=1}^{n} z_j.(M - z_j) \tag{5.3}$$

onde z_j *representa o número de n-uplas em* A_ψ *que tem 0 na j-ésima posição para todo* j, $j \in \{1, 2, \cdots, n\}$, M *denota a cardinalidade de* A_ψ *e* d *denota a mínima distância de Hamming neste conjunto.*

Exemplo 5.3. *Para o estado* $|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$ *temos que* $A_\psi = \{000, 011, 110, 101\}$*. Logo* $M = 4$, $z_1, z_2, z_3 = 2$ *e substituindo na equação (5.3), temos:*

$$Q(|\psi_{HGHZ}\rangle) \equiv Q'(|\psi_{HGHZ}\rangle) = \frac{4}{3}.\frac{1}{4^2}\sum_{j=1}^{3} z_j.(4 - z_j) = \frac{1}{12}.(4 + 4 + 4) = 1.$$

Teorema 5.2. *Seja* $|\psi\rangle$ *um estado quântico puro com amplitudes iguais a* $\frac{1}{\sqrt{M}}$*, cujo* A_ψ *associado satisfaz* $d > 1$ *e tem cardinalidade M. Então,* $|\psi\rangle$ *é um estado quântico puro de máximo emaranhamento global se, e somente se,* $z_j = \frac{M}{2}$ *para todo* $j \in 1, 2, \cdots, n$*.*

Portanto, dado um estado quântico puro $|\psi\rangle$ com amplitudes iguais a $\frac{1}{\sqrt{M}}$, composto por M-kets e cujo conjunto A_ψ é caracterizado por $d > 1$, então este estado satisfaz $Q = 1$ se, e somente se, $z_j = \frac{M}{2}$ para todo $j \in 1, 2, \cdots, n$. Esta é uma condição que nos permite classificar estados de máximo emaranhamento global (GAZZONI, 2008).

5.3 Mapeamento por Particionamento de Conjuntos

Dado um conjunto $\mathbf{S}$, um particionamento L-nível de $\mathbf{S}$ é definido como uma sequência de $L+1$ partições $\Gamma_0, \cdots, \Gamma_L$ tal que (IMAI; HIRAKAWA, 1977; UNGER-BOEK, 1982):

- a partição do nível 0 consiste no conjunto $\mathbf{S}$ completo, isto é, $\Gamma_0 = \{\mathbf{S}\}$.
- a partição Γ_l é um refinamento da partição Γ_{l-1}, para $l = 1, \cdots, L$.
- a partição do nível L consiste nos subconjuntos unitários de $\mathbf{S}$, isto é, $\Gamma_L = \{\{s\} : s \in \mathbf{S}\}$.

Definição 5.3. *Dado um conjunto $\boldsymbol{S}$, uma **partição** de $\boldsymbol{S}$ consiste em uma coleção $\Gamma = \{\boldsymbol{S}_1, \cdots, \boldsymbol{S}_p\}$ de p subconjuntos não vazios de $\boldsymbol{S}$ tais que:*

- *a união de todos os elementos da partição é igual ao conjunto $\boldsymbol{S}$, isto é, $\boldsymbol{S}_1 \cup \cdots \cup \boldsymbol{S}_p = \boldsymbol{S}$.*
- *a interseção de quaisquer dois elementos da partição é vazia, isto é, $\boldsymbol{S}_i \cap \boldsymbol{S}_j = \oslash$, $i \neq j$.*

Observação 5.3. *Uma partição Γ' é dita ser um **refinamento** de outra partição Γ se todo elemento de Γ' é um subconjunto de algum elemento de Γ.*

Definição 5.4. *A **distância de subespaço intrasubset** do nível l é definida por*

$$d_s^{(l)} = min\{d_s(\mathcal{X}) : \mathcal{X} \in \Gamma_l\}$$

para $l = 0, \cdots, L$. Em particular, $d_s^{(0)} = d_s(\boldsymbol{S})$ e $d_s^{(L)} = \infty$.

Observação 5.4. *Neste contexto a construção multinível sempre será aninhada, ou seja, cada nó pai do nível anterior tem o mesmo número de nó filhos, no caso 2 filhos, do nível posterior, assim tais níveis devem ser "protegidos"por códigos clássicos de comprimento n sobre $\mathbb{Z}_2$, chamados **códigos componentes** e denotados por H_l, com distâncias (de Hamming) mínimas $d_H^{(l)} = d_H(H_l)$. Por (CALDERBANK, 1989) a distância mínima do código quântico de subespaço projetado é limitada inferiormente por:*

$$d_S(C) \geq min\{d_S^{(l-1)}.\ d_H^{(l)} : 1 \leq l \leq L'\}.$$

Observação 5.5. *Como $\boldsymbol{S}$ é um código de subespaço tal que dois a dois subespaços em uma grassmanniana tenham interseção nula, segue que a propriedade de que a distância de subespaço terá que ser máxima, ou equivalentemente, que a distância de subespaço entre quaisquer dois subespaços é invariante, ou seja, $d_S^{(0)} = d_S^{(1)} = \cdots = d_S^{(l-1)}$ para $l = 0, \cdots, L$, tem que ser satisfeita.*

5.4 Proposta de Rotulamento Associado ao Estado Quântico Separável Universal

A proposta consiste em particionar um conjunto Γ_0 (código de subespaço com máxima distância de subespaço) $\Gamma_0 = \mathcal{C} \subset \mathbf{S} \subset \mathbb{P}(\mathbb{F}_2^m)$ em L-níveis e associar aos elementos do conjunto A_ψ, ou seja, o mapeamento por particionamento de conjuntos é uma forma de rotulamento de Γ_0. Seja $\Gamma_0, \cdots, \Gamma_L$ tal particionamento. Apresentamos a seguir algumas definições e resultados que mostram a existência do código de subespaço com a máxima distância de subespaço $\Gamma_0 = \mathcal{C}$ (ETZION; RAVIV, 2015; ETZION; STORME, 2016).

Definição 5.5. *Dois subespaços $X, Y \in \mathcal{G}_q(m,k)$ são **disjuntos** se sua interseção é o espaço nulo, ou seja, $X \cap Y = 0$.*

Definição 5.6. *Um **partial k-spread** ou **partial spread** em $\mathcal{G}_q(m,k)$ é um conjunto de subespaços disjuntos de $\mathcal{G}_q(m,k)$.*

Observação 5.6. *Se k divide m e o partial spread tem $\frac{q^m-1}{q^k-1}$ subespaços então o partial spread é chamado **k-spread** ou simplesmente **spread**.*

Definição 5.7. *O **número** de k-subespaços no maior partial spread de $\mathcal{G}_q(m,k)$ será denotado por $E_q[m,k]$.*

Teorema 5.3. *Se k divide m então $E_q[m,k] = \frac{q^m-1}{q^k-1}$.*

Observação 5.7. *O Teorema 5.3 é central na proposta em consideração, pois garante a existência do código de subespaço $\mathcal{C}$. A demonstração do referido teorema encontra-se em (ETZION; VARDY, 2011).*

Exemplo 5.4. *Considere $\mathcal{G}_2(4,2)$. O número de subespaços com a máxima distância de subespaço, nesse caso d=4, é dado por $E_2[4,2] = \frac{2^4-1}{2^2-1} = \frac{15}{3} = 5$. Se $X, Y \in \mathcal{S} \subset \mathcal{G}_q(m,k)$ são dois subespaços quaisquer disjuntos, então $d(X,Y) = dimX + dimY - 2.dim(X \cap Y) = 2 + 2 - 2.0 = 4$.*

Exemplo 5.5. *Considere $\mathcal{G}_2(6,3)$. O número de subespaços com a máxima distância de subespaço, nesse caso d=6, é dado por $E_2[6,3] = \frac{2^6-1}{2^3-1} = \frac{63}{7} = 9$.*

Exemplo 5.6. *Considere $\mathcal{G}_2(m, k = \frac{m}{2})$. O número de subespaços com a máxima distância de subespaço, nesse caso d=m, é dado por $E_2[m,k] = \frac{2^m-1}{2^k-1} = \frac{(2^k)^2-1^2}{2^k-1} = \frac{(2^k-1)(2^k+1)}{2^k-1} = 2^k + 1$.*

Observação 5.8. *Como existem $|\mathcal{S}| = 2^k + 1$ subespaços com a máxima distância de subespaço em $\mathcal{G}_2(m, k = \frac{m}{2})$, segue que para utilizar o mapeamento por particionamento de conjuntos na proposta em consideração a cardinalidade de $\mathcal{C}$ tem que ser 2^k, ou seja, precisamos escolher 2^k subespaços dentre os $2^k + 1$ possíveis.*

Definição 5.8. *Um* ***sunflower*** $\mathcal{S} \subset \mathcal{G}_q(m,k)$ *é um código equidistante t-interseção quando quaisquer duas palavras-código* $X, Y \in \mathcal{S}$ *interceptam em algum t-subespaço* $\mathcal{Z}$*.*

Definição 5.9. *O t-subespaço* $\mathcal{Z}$ *é chamado* ***centro*** *de* $\mathcal{S}$ *e é denotado por* $Cen(\mathcal{S})$*.*

Exemplo 5.7. *Considere o código* $\mathcal{S} = \{S_1, S_2, S_3\}$ *de* $\mathcal{G}_2(4,2)$ *onde*

$S_1 = \{0000, 0001, 1000, 1001\}$, $S_2 = \{0000, 0001, 0100, 0101\}$, $S_3 = \{0000, 0001, 0010, 0011\}$.

Observe que $S_1 \cap S_2 \cap S_3 = \{0000, 0001\} = \mathcal{Z}$*. Portanto, dizemos que* $\mathcal{S}$ *é um código sunflower 1-interseção e o centro de* $\mathcal{S}$ *é* $Cen(\mathcal{S}) = \{0000, 0001\}$*.*

Observação 5.9. *Um partial spread é claramente um 0-interseção sunflower.*

Observação 5.10. *Existe uma relação estreita entre códigos clássicos e códigos de subespaços na grassmanniana, por meio do conceito conhecido por* ***q-analog*** *(é uma estrutura matemática parametrizada por uma quantidade q que generaliza uma estrutura também conhecida e chamada* ***q-extensão*** *ou* ***q-generalização****). No caso em consideração o q-analog substitui subconjuntos por subespaços em* $\mathbb{P}(\mathbb{F}_2^m)$ *e suas cardinalidades pelas dimensões dos subespaços em questão. Podemos destacar (ETZION; RAVIV, 2015): 1) a distância de Hamming está para o hipercubo de Hamming assim como a distância de subespaço esta para o diagrama de Hasse do espaço projetivo, 2) um código binário de peso constante w é chamado sunflower se quaisquer duas palavras-código se interceptam em t-coordenadas, e 3) um partial spread em* $\mathcal{G}_q(m,k)$ *é q-analog de um código de peso constante 0-interseção de comprimento m e peso k.*

Observação 5.11. *Observe na Figura 19 que existem 5 subespaços (mostrados em "vermelho") formando um código sunflower 0-interseção ou partial 2-spread,* $\mathcal{S} \subset \mathcal{G}_2(4,2)$ *Portanto, escolhemos 4 subespaços para compor o código de subespaço* $\mathcal{C} \subset \mathcal{S}$*. Desse modo, existem 5 conjuntos de subespaços e cada conjunto contém 7 subespaços totalizando os 35 existentes na grassmanniana* $\mathcal{G}_2(4,2)$*. Desse modo, escolhemos 4 dos 5 conjuntos de subespaços possíveis e depois selecionamos um representante de cada conjunto para compor o código* $\mathcal{C}$*.*

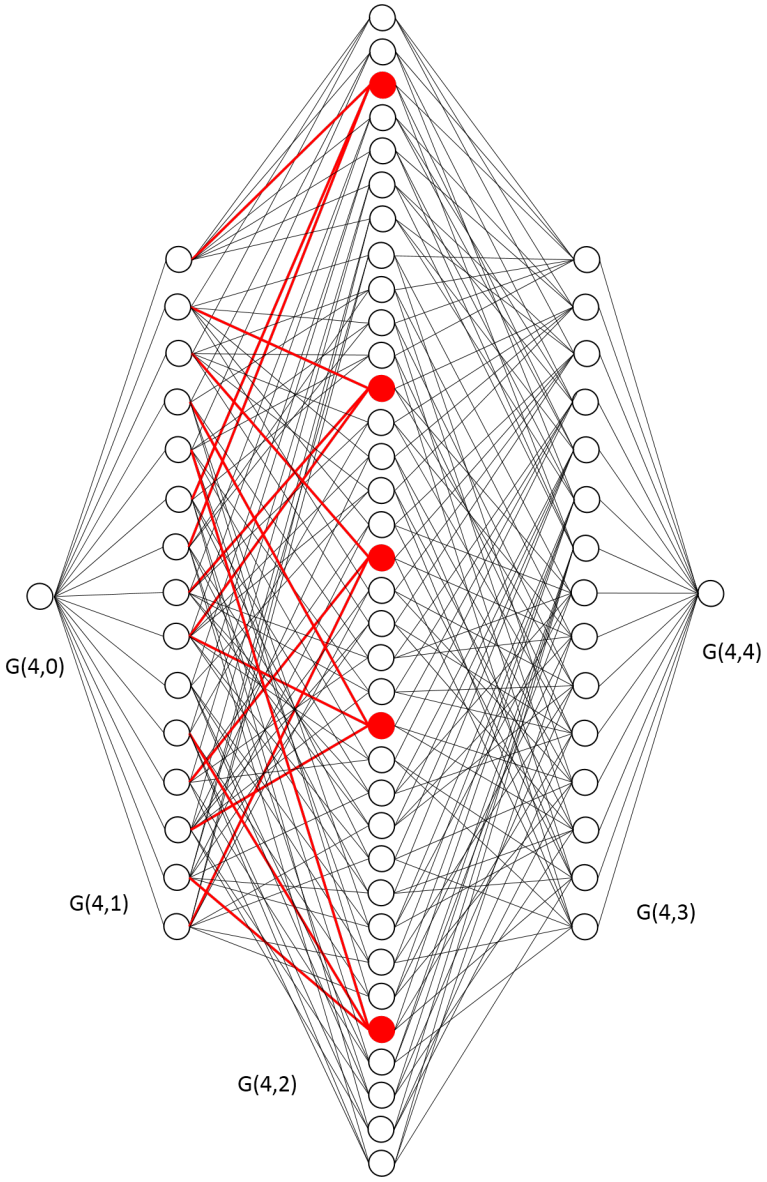


Figura 19 – Sunflower 0-Interseção ou Partial 2-Spread

Apresentamos, a seguir, alguns exemplos de códigos quânticos de subespaços concatenados de modo que os parâmetros de tais códigos são dados por (N, M, d, k), onde M é o produto das cardinalidades dos códigos componentes clássicos utilizado na proteção, k é a soma dos digítos de informação $k_i's$ utilizado nos códigos componentes clássicos e a distância mínima d é a menor dentre o produto entre as distâncias de subespaços dos níveis e as distâncias mínimas dos códigos componentes clássicos de cada nível. E N é o comprimento das palavras-código dos códigos componentes.

Exemplo 5.8. *Considere o espaço projetivo* $\mathbb{P}(\mathbb{F}_2^4)$. *O código de subespaço* $\mathcal{C} = \{S_1, S_2, S_3, S_4\}$, *onde:*

$$S_1 = \{0000, 0010, 0001, 0011\} = \langle 0010, 0001 \rangle$$

$$S_2 = \{0000, 1000, 0100, 1100\} = \langle 1000, 0100 \rangle$$

$$S_3 = \{0000, 1010, 0101, 1111\} = \langle 1010, 0101 \rangle$$

$$S_4 = \{0000, 1011, 0111, 1101\} = \langle 1011, 0111 \rangle,$$

possui parâmetros $(m, M, d, k) = (4, 4, 4, 2)$*, onde* m *é a dimensão do espaço projetivo,* M *é a cardinalidade do código de subespaço,* d *é a distância mínima de subespaço e* k *é a dimensão da grassmanniana.*

A seguir, apresentamos o mapeamento por particionamento de conjuntos do código $\mathcal{C}$ *que contêm 4 subespaços, onde podemos associar o código de subespaço a um estado quântico puro separável universal, fazendo a leitura de baixo pra cima:*

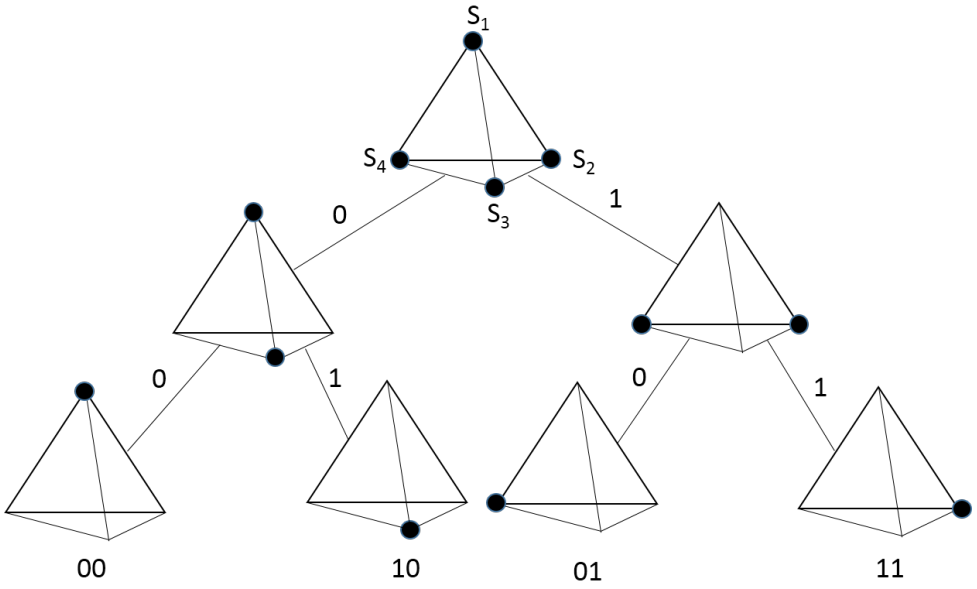


Figura 20 – Rotulamento de Código de Órbita ou Cíclico de Subespaço

$$S_1 \sim 00, \quad S_2 \sim 11, \quad S_3 \sim 10, \quad S_4 \sim 01.$$

Portanto, o particionamento binível $\Gamma_0,\ \Gamma_1,\ \Gamma_2$ *de* $\boldsymbol{S}$ *é dado por:*

$$\Gamma_0 = \{\{S_1, S_2, S_3, S_4\}\}$$

$$\Gamma_1 = \{\{S_1, S_3\}, \{S_2, S_4\}\}$$

$$\Gamma_2 = \{\{S_1\}, \{S_2\}, \{S_3\}, \{S_4\}\}$$

Esse rotulamento permite caracterizar um estado quântico puro separável universal de 2 q-bits $|\psi\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle$*. Supondo que se deseja um código quântico de subespaço com distância mínima d=8, é necessário encontrar códigos componentes binários* $\mathcal{H}_1$*,* $\mathcal{H}_2$ *(pois* $p_1 = p_2 = 2$*) de distância mínima de Hamming pelo menos* $d = 2$*. Neste exemplo, tomemos* $\mathcal{H}_1 = \mathcal{H}_2 = \{0000, 0011, 1100, 1111\}$*, com parâmetros* $(n, k, d) = (4, 2, 2)$*. Como*

$d_s^{(0)} = d_s^{(1)} = 4$, *o objetivo foi alcançado, ou seja,* $d = 8$. *Para determinar as palavras-código, formam-se todas as possíveis matrizes, onde cada matriz é do tipo* L' *linhas por* n *colunas, contendo as possíveis palavras-código de* $\mathcal{H}_l$ *na* l*-ésima linha. O conjunto de todas essas matrizes é denotado por* $\mathcal{A}$ *e tem cardinalidade* $|\mathcal{A}| = |\mathcal{H}_1|\cdots|\mathcal{H}_{L'}| = M$. *Cada matriz* $\boldsymbol{A} \in \mathcal{A}$ *pode resultar em mais de uma palavra-código. Portanto, para este exemplo, teremos na primeira linha as palavras-código do código* $\mathcal{H}_1$ *e na segunda linha as palavras-código do código* $\mathcal{H}_2$, *todas as combinações possíveis são representadas pelas matrizes:*

$$\mathcal{A} = \left\{ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \cdots, \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \cdots, \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \right\}.$$

e a cardinalidade é $|\mathcal{A}| = |\mathcal{H}_1|.|\mathcal{H}_2| = 16$. *Neste caso, cada matriz de* $\mathcal{A}$ *dá origem a uma única palavra-código. A matriz*

$$\boldsymbol{A} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

dá origem à palavra-código

$$(S_4, S_4, S_3, S_3),$$

descrita pelos caminhos, (0,1) e (1,0) identificados pelas colunas de $\boldsymbol{A}$. *Neste exemplo os parâmetros do código quântico de subespaço concatenado é* $(N, M, d, k) = (N, 16, 8, 4)$.
Assim, um estado quântico de máximo emaranhamento global é dado pelo código $\mathcal{C} = \{00, 11\}$ *(GAZZONI, 2008), podemos associar ao código de subespaço* $\mathcal{C}_1 = \{S_1, S_2\} \equiv \{00, 11\}$.
Sendo assim, podemos utilizar os códigos de subespaços n-shot para obter estado quântico puro de máximo emaranhamento global!?

- *Estendendo o código de subespaço* $\mathcal{C}_1$ *para o 2-shot, temos:*

  $$\boldsymbol{\mathcal{C}_1} = \mathcal{C}_1 \times \mathcal{C}_1 = \{S_1S_1, S_1S_2, S_2S_1, S_2S_2\}.$$

  Os parâmetros do código $\boldsymbol{\mathcal{C}_1}$ *são* $(m.n, M^n, d, k.n) = (8, 4, 4, 4)$. *Associando:*

  $$S_1S_1 \sim 0000, \quad S_1S_2 \sim 0011, \quad S_2S_1 \sim 1100, \quad S_2S_2 \sim 1111,$$

  segue que $|\psi\rangle = \frac{1}{\sqrt{4}}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$.

  Assim, será que esse estado é de máximo emaranhamento global?

  $$Q'(|\psi\rangle) = \frac{4}{4}.\frac{1}{4^2}\sum_{j=1}^{4} z_j.(4 - z_j) = \frac{1}{16}.(2.2 + 2.2 + 2.2 + 2.2) = \frac{1}{16}.4.2.2 = 1,$$

  onde n=4, M=4 e $z_j = 2$ *para j=1,2,3,4.*

- *Estendendo agora o código de subespaço $\mathcal{C}_1$ para o 3-shot, temos:*

  $\boldsymbol{\mathcal{C}_1} = \mathcal{C}_1 \times \mathcal{C}_1 \times \mathcal{C}_1 = \{S_1S_1S_1, S_1S_1S_2, S_1S_2S_1, S_2S_1S_1, S_2S_2S_1, S_1S_2S_2, S_2S_1S_2, S_2S_2S_2\}$.

  Os parâmetros do código $\boldsymbol{\mathcal{C}_1}$ são $(m.n, M^n, d, k.n) = (12, 8, 4, 6)$. Associando:

  $$S_1S_1S_1 \sim 000000, \quad S_1S_1S_2 \sim 000011, \quad S_1S_2S_1 \sim 001100, \quad S_2S_1S_1 \sim 110000,$$

  $$S_2S_1S_2 \sim 110011, \quad S_2S_2S_1 \sim 111100, \quad S_1S_2S_2 \sim 001111, \quad S_2S_2S_2 \sim 111111,$$

  segue que $|\psi\rangle = \frac{1}{\sqrt{8}}(|000000\rangle + |000011\rangle + \cdots + |111111\rangle)$.

  Assim será que esse estado é de máximo emaranhamento global?

  $$Q'(|\psi\rangle) = \frac{4}{6}.\frac{1}{8^2}\sum_{j=1}^{6} z_j.(8 - z_j) = \frac{2}{3}.\frac{1}{64}.(4.4 + 4.4 + \cdots + 4.4) = \frac{2}{3}.\frac{1}{64}.6.4.4 = 1,$$

  onde n=6, M=8 e $z_j = 4$ para $j = 1, 2, 3, \cdots, 6$.

Exemplo 5.9. *Se no Exemplo 5.8 substituirmos os códigos componentes por:*

$$\mathcal{H}_1 = \{0000, 0011, 1100, 1111\},$$

com parâmetros $(n, k, d) = (4, 2, 2)$ e,

$$\mathcal{H}_2 = \{0000, 1111\},$$

com parâmetros $(n, k, d) = (4, 1, 4)$, obtemos um outro código quântico de subespaço concatenado com parâmetros $(N, M, d, k) = (N, 8, 8, 3)$, onde as palavras-código são:

$$\mathcal{A} = \left\{ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \right\}.$$

Exemplo 5.10. *Considere o espaço projetivo $\mathbb{P}(\mathbb{F}_2^6)$. O código $\mathcal{C} = \{S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8\}$, onde:*

$$S_1 = \langle 000100, 000010, 000001\rangle \quad S_2 = \langle 100000, 010000, 001000\rangle$$

$$S_3 = \langle 100001, 010010, 001100\rangle \quad S_4 = \langle 100010, 010100, 001011\rangle$$

$$S_5 = \langle 100011, 010110, 001111\rangle \quad S_6 = \langle 100100, 010011, 001110\rangle$$

$$S_7 = \langle 100110, 010001, 001010\rangle \quad S_8 = \langle 100110, 010111, 001101\rangle,$$

é um subconjunto sunflower 0-interseção ou partial 3-spread $\mathcal{C} \subset \mathcal{S} \subset \mathcal{G}_2(6, 3)$ com parâmetros $(m, M, d, k) = (6, 8, 6, 3)$, onde m é a dimensão do espaço projetivo, M é a

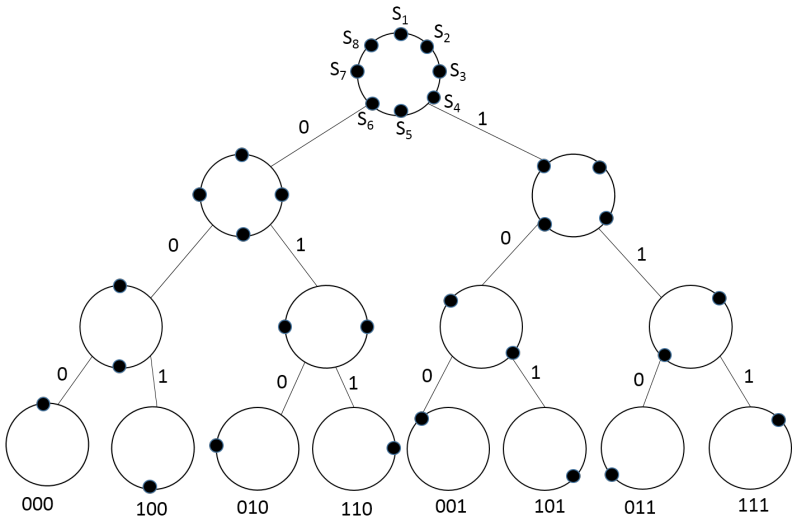


Figura 21 – Rotulamento de Código de Órbita ou Cíclico de Subespaço

cardinalidade do código de subespaço, d é a distância mínima de subespaço e k é a dimensão da Grasmmaniana.

Apresentamos o mapeamento por particionamento de conjuntos do código $\mathcal{C}$ que contêm 8 subespaços, onde podemos associar o código de subespaços a um estado quântico puro separável universal, fazendo a leitura de baixo pra cima:

$$S_1 \sim 000, \quad S_2 \sim 111, \quad S_3 \sim 110, \quad S_4 \sim 101$$

$$S_5 \sim 100, \quad S_6 \sim 011, \quad S_7 \sim 010, \quad S_8 \sim 001.$$

Portanto, o particionamento Trinível $\Gamma_0,\ \Gamma_1,\ \Gamma_2,\ \Gamma_3$ de $\boldsymbol{S}$ é dado por:

$$\Gamma_0 = \{\{S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8\}\}$$

$$\Gamma_1 = \{\{S_1, S_3, S_5, S_7\}, \{S_2, S_4, S_6, S_8\}\}$$

$$\Gamma_2 = \{\{S_1, S_5\}, \{S_3, S_7\}, \{S_4, S_8\}, \{S_2, S_6\}\}$$

$$\Gamma_3 = \{\{S_1\}, \{S_2\}, \{S_3\}, \{S_4\}, \{S_5\}, \{S_6\}, \{S_7\}, \{S_8\}\}.$$

Esse rotulamento permite caracterizar um estado quântico puro separável universal de 3 q-bits $|\psi\rangle = |000\rangle + |001\rangle + |010\rangle + |100\rangle + |110\rangle + |101\rangle + |011\rangle + |111\rangle$. Supondo que se deseja um código quântico de subespaço concatenado com distância mínima d=18, é necessário encontrar códigos componentes binários $\mathcal{H}_1 = \mathcal{H}_2 = \mathcal{H}_3$ (pois $p_1 = p_2 = p_3 = 2$) de distância mínima de Hamming pelo menos $d = 3$. Observe que os códigos componentes não necessariamente precisam serem iguais. Neste exemplo, $\mathcal{H}_1 = \mathcal{H}_2 = \mathcal{H}_3 = \{000000, 010101, 110011, 001111, 100110, 011010, 111100, 101001\}$, com parâmetros $(n, k, d) = (6, 3, 3)$. Como $d_s^{(0)} = d_s^{(1)} = d_s^{(2)} = 6$, o objetivo foi alcançado, ou seja, d=18. O conjunto de todas as matrizes que formam as palavras-código é denotado por $\mathcal{A}$ e tem

cardinalidade $|\mathcal{A}| = |\mathcal{H}_1|\cdots|\mathcal{H}'_L| = M$. *Cada matriz* $\boldsymbol{A} \in \mathcal{A}$ *pode resultar em mais de uma palavra-código.*
Neste exemplo as possíveis matrizes são:

$$\mathcal{A} = \left\{ \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix}, \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&1&0&1&1&1 \end{bmatrix}, \cdots, \begin{bmatrix} 0&0&1&1&1&1\\ 0&0&1&1&1&1\\ 0&0&1&1&1&1 \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} 1&0&0&1&1&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix}, \begin{bmatrix} 1&0&0&1&1&0\\ 0&0&0&0&0&0\\ 1&0&1&0&0&1 \end{bmatrix}, \cdots, \begin{bmatrix} 1&0&1&0&0&1\\ 1&0&1&0&0&1\\ 1&0&1&0&0&1 \end{bmatrix} \right\},$$

e a cardinalidade é $|\mathcal{A}| = |\mathcal{H}_1|.|\mathcal{H}_2|.|\mathcal{H}_3| = 8.8.8 = 512 = M$. *Neste caso, cada matriz de* $\mathcal{A}$ *dá origem a uma única palavra-código, assim os parâmetros do código quântico de subespaço concatenado são* $(N, M, d, k) = (N, 512, 18, 9)$. *A matriz*

$$\boldsymbol{A} = \begin{bmatrix} 0&0&1&1&1&1\\ 1&0&0&1&1&0\\ 1&0&1&0&0&1 \end{bmatrix}$$

dá origem à palavra-código

$$(S_3, S_1, S_4, S_6, S_6, S_4),$$

descrita pelos caminhos, (0,1,1), (0,0,0), (1,0,1) e (1,1,0) idendificados pelas colunas de $\boldsymbol{A}$.

Neste caso, $\mathcal{C}_1 = \{S_1, S_3, S_4, S_6\}$ *é um código associado ao estado quântico de máximo emaranhamento global* $|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$. *Portanto, podemos usar os códigos de subespaços n-shot para obter estado quântico puro de máximo emaranhamento global!*

- *Estendendo o código de subespaço* $\mathcal{C}_1$ *para o 2-shot, temos:*

$$\boldsymbol{\mathcal{C}_1} = \mathcal{C}_1 \times \mathcal{C}_1 = \{S_1S_1, S_1S_3, S_1S_4, \ldots, S_6S_6\}.$$

Os parâmetros do código $\boldsymbol{\mathcal{C}_1}$ *são* $(m.n, M^n, d, k.n) = (12, 16, 6, 6)$. *Associando:*

$$S_1S_1 \sim 000000, \quad S_1S_3 \sim 000110, \quad S_1S_4 \sim 000101, \quad S_1S_6 \sim 000011,$$

$$S_3S_1 \sim 110000, \quad S_3S_3 \sim 110110, \quad S_3S_4 \sim 110101, \quad S_3S_6 \sim 110011,$$

$$S_4S_1 \sim 101000, \quad S_4S_3 \sim 101110, \quad S_4S_4 \sim 101101, \quad S_4S_6 \sim 101011,$$

$$S_6S_1 \sim 011000, \quad S_6S_3 \sim 011110, \quad S_6S_4 \sim 011101, \quad S_6S_6 \sim 011011,$$

segue que

$$|\psi\rangle = \frac{1}{\sqrt{16}}(|000000\rangle + |000110\rangle + \cdots + |011011\rangle).$$

Será que esse estado é emaranhado global?

$$Q'(|\psi\rangle) = \frac{4}{6}.\frac{1}{16^2}\sum_{j=1}^{6} z_j.(16 - z_j) = \frac{2}{3}.\frac{1}{256}.(6.6 + 6.6 + \cdots + 6.6) = \frac{2}{3}.\frac{1}{256}.6.8.8 = 1,$$

onde n=6, M=16 e $z_j = 8$, para $j = 1, 2, 3, \cdots, 6$. Portanto $|\psi\rangle$ é um estado emaranhado global! Logo, a partir da associação de estado de máximo emaranhamento global a um código de subespaço, podemos utilizar o código de subespaço n-shot para produzir uma nova classe de estados quânticos de máximo emaranhamento global.

O código $\mathcal{C}_2 = \{S_1, S_2\}$ é associado ao estado quântico de máximo emaranhamento global $|\psi\rangle = |000\rangle + |111\rangle)$. Usando os códigos de subespaços n-shot, podemos obter estados quânticos puro emaranhado global!

- *Estendendo o código de subespaço $\mathcal{C}_2$ para o 2-shot, segue que*

$$\boldsymbol{\mathcal{C}_2} = \mathcal{C}_2 \times \mathcal{C}_2 = \{S_1S_1, S_1S_2, S_2S_1, S_2S_2\}.$$

Os parâmetros do código $\boldsymbol{\mathcal{C}_2}$ são $(m.n, M^n, d, k.n) = (12, 4, 6, 6)$. Associando

$$S_1S_1 \sim 000000, \quad S_1S_2 \sim 000111, \quad S_2S_1 \sim 111000, \quad S_2S_2 \sim 111111,$$

segue que $|\psi\rangle = \frac{1}{\sqrt{4}}(|000000\rangle + |000111\rangle + |111000\rangle + |111111\rangle)$. Será que esse estado é emaranhado global?

$$Q'(|\psi\rangle) = \frac{4}{6}.\frac{1}{4^2}\sum_{j=1}^{6} z_j.(4 - z_j) = \frac{2}{3}\frac{1}{16}.(2.2+2.2+2.2+2.2+2.2+2.2) = \frac{2}{3}\frac{1}{16}.6.2.2 = 1,$$

onde n=6, M=4 e $z_j = 2$, para $j = 1, 2, \cdots, 6$.

Proposição 5.2. *Seja $\mathbb{P}(\mathbb{F}_2^m)$ o espaço projetivo e seja um código de subespaço $\mathcal{C} \subset \mathcal{S} \subset \mathcal{G}_q(m, k = \frac{n}{2})$ cuja cardinalidade é $|\mathcal{C}| = 2^k$. Obtemos por meio do mapeamento de particionamento de conjuntos para 2^k subespaços, uma forma de descrever um estado quântico puro separável universal de n q-bits, e assim, obter códigos quânticos de subespaços concatenados com parâmetros (N, M, d, K). Além disso, podemos descrever estados quânticos de máximo emaranhamento global e também utilizar os códigos de subespaço n-shot para descrever novos estados quânticos de máximo emaranhamento global.*

5.5 Proposta de Rotulamento Associado Diretamente a Estados Quânticos de Máximo Emaranhamento Global

Nesta proposta faremos a associação direta entre um estado quântico de máximo emaranhamento global e o mapeamento por partionamento de conjuntos via uma matriz dos códigos Reed-Muller.

Códigos Reed-Muller formam uma classe de códigos lineares sobre $\mathbb{F}_2$ tal que a codificação e a decodificação são simples de serem descritas. Para cada valor de m e de r tal que $r < m$ existe um código Reed-Muller de comprimento 2^m chamado código Reed-Muller de r-ésima ordem. A matriz geradora do código de Reed-Muller de r-ésima ordem e de comprimento 2^m é definida como:

$$G = \begin{bmatrix} G_0 \\ G_1 \\ \vdots \\ G_r \end{bmatrix},$$

onde G_0 é um vetor de comprimento $n = 2^m$ contendo apenas 1's; G_1 é uma matriz $m \times 2^m$ tendo nas colunas todas as m-uplas binárias e G_l é contruída de G_1 considerando todos os produtos das linhas de G_1. Por conveniência de representação de G_1, considere-se as colunas mais a esquerda como sendo toda nula, a coluna mais a direita como toda 1 e as intermediárias como sendo n-uplas binárias, representando inteiro em ordem crescente. Os parâmetros do código Reed-Muller são (n, k, d), onde o comprimento é $n = 2^m$, a dimensão é $k = \binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r}$ e a distância mínima é $d = 2^{m-r}$.

Exemplo 5.11. *Considerando m=3, segue que,* $n = 2^m = 2^3 = 8$, $k = \binom{3}{0} + \binom{3}{1} + \ldots + \binom{3}{r}$ *e* $d = 2^{m-r}$. *Portanto, para r=0, obtemos um código Reed-Muller de ordem zero com parâmetros* $(n, k, d) = (8, 1, 8)$, *cuja matriz geradora é:*

$$G = \begin{bmatrix} G_0 \end{bmatrix} = [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1].$$

Para r=1, obtemos um código Reed-Muller de primeira ordem com parâmetro $(n, k, d) = (8, 4, 4)$, *cuja matriz geradora é:*

$$G = \begin{bmatrix} G_0 \\ G_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix},$$

onde $G_0 = [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1]$ *e* $G_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$.

Apresentamos, a seguir, uma forma de rotular um estado quântico de máximo emaranhamento global utilizando o mapeamento por particionamento de conjuntos via a matriz G_1 modificada do código Reed-Muller.

Exemplo 5.12. *Considere o particionamento obtido no Exemplo 5.8 e seja a matriz:*

$$G_1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

de um código Reed-Muller com $m = 2$, ou seja, de comprimento $n = 2^2 = 4$. Eliminando a primeira coluna de G_1 obtemos uma matriz G_1 modificada com dois geradores $\langle 011, 101\rangle$ que dão origem ao código $\mathcal{C} = \{000, 011, 101, 110\}$ que está associado ao estado quântico de máximo emaranhamento global $|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$. Para rotularmos o código de subespaço do Exemplo 5.8 associando ao estado quântico de máximo emaranhamento global $|\psi_{HGHZ}\rangle$ basta efetuarmos uma multiplicação de matrizes entre os rótulos obtidos no Exemplo 5.8 e a matriz G_1 modificada. Como,

$$S_1 \sim 00, \quad S_2 \sim 11, \quad S_3 \sim 10, \quad S_4 \sim 01,$$

segue que

$$(0\ 0).\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = (0\ 0\ 0), \qquad (0\ 1).\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = (1\ 0\ 1),$$

$$(1\ 0).\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = (0\ 1\ 1), \qquad (1\ 1).\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = (1\ 1\ 0).$$

Portanto, o rotulamento associando um código de subespaço ao estado quântico de máximo emaranhamento global é dado por:

$$S_1 \sim 000, \quad S_2 \sim 110, \quad S_3 \sim 011, \quad S_4 \sim 101.$$

Com isso, o estado quântico de máximo emaranhamento global $|\psi_{HGHZ}\rangle$ é descrito da seguinte forma:

$$|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}(|S_1\rangle + |S_3\rangle + |S_4\rangle + |S_2\rangle).$$

Exemplo 5.13. *Considere, agora, o particionamento obtido no Exemplo 5.10 e considere a matriz:*

$$G_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Eliminando a primeira coluna de G_1 obtemos uma matriz G_1 modificada com três geradores $\langle 0001111, 0110011, 1010101\rangle$ que dão origem ao código,

$$\mathcal{C} = \{0000000, 0001111, 0110011, 1010101, 0111100, 1011010, 11001100, 1101001\},$$

que está associado ao estado quântico de máximo emaranhamento global

$$|\psi_{Simplex}\rangle = \frac{1}{\sqrt{8}}(|0000000\rangle + |0001111\rangle + |0110011\rangle + |1010101\rangle + |0111100\rangle + |1011010\rangle$$

$$+|1100110\rangle + |1101001\rangle).$$

Para rotularmos o código de subespaço do Exemplo 5.10 associando ao estado quântico de máximo emaranhamento global $|\psi_{Simplex}\rangle$ *basta efetuarmos uma multiplicação de matrizes entre os rótulos obtidos no Exemplo 5.10 e a matriz* G_1 *modificada. Como,*

$$S_1 \sim 000, \quad S_2 \sim 111, \quad S_3 \sim 110, \quad S_4 \sim 101$$

$$S_5 \sim 100, \quad S_6 \sim 011, \quad S_7 \sim 010, \quad S_8 \sim 001,$$

segue que

$$(0\ 0\ 0).\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = (0\ 0\ 0\ 0\ 0\ 0\ 0),$$

$$(0\ 0\ 1).\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = (1\ 0\ 1\ 0\ 1\ 0\ 1),$$

$$(0\ 1\ 0).\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = (0\ 1\ 1\ 0\ 0\ 1\ 1),$$

$$(1\ 0\ 0).\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = (0\ 0\ 0\ 1\ 1\ 1\ 1),$$

$$(1\ 1\ 0).\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = (0\ 1\ 1\ 1\ 1\ 0\ 0),$$

$$(1\ 0\ 1).\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = (1\ 0\ 1\ 1\ 0\ 1\ 0),$$

$$(0\ 1\ 1).\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = (1\ 1\ 0\ 0\ 1\ 1\ 0),$$

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

Portanto, o rotulamento associando um código de subespaço ao estado quântico de máximo emaranhamento global é dado por:

$$S_1 \sim 0000000, \quad S_2 \sim 1101001, \quad S_3 \sim 0111100, \quad S_4 \sim 1011010.$$

$$S_5 \sim 0001111, \quad S_6 \sim 1100110, \quad S_7 \sim 0110011, \quad S_8 \sim 1010101.$$

Com isso, o estado quântico de máximo emaralhamento global $|\psi_{Simplex}\rangle$ *é descrito da seguinte maneira:*

$$|\psi_{Simplex}\rangle = \frac{1}{\sqrt{8}}(|S_1\rangle + |S_5\rangle + |S_7\rangle + |S_8\rangle + |S_3\rangle + |S_4\rangle + |S_6\rangle + |S_2\rangle).$$

Proposição 5.3. *Seja a matriz* G_1 *definida no código de Reed-Muller. A eliminação da primeira coluna da origem a uma matriz* G_1 *modificada do tipo* $m \times 2^m - 1$*, cujas linhas são os geradores que estão associados a um código clássico de parâmetros* $(2^m - 1, m, 2^{m-1})$ *cujas palavras-código estão associadas a um estado quântico de máximo emaranhamento global. Por meio do mapeamento por particionamento de conjuntos associamos um código de subespaço com a máxima distância de subespaço a um estado quântico de máximo emaranhamento global através da multiplicação das matrizes dos rótulos do particionamento pela* G_1 *modificada obtendo assim um código quântico de subespaço.*

Conclusões e Perspectivas de Pesquisa

Esperamos que este trabalho possa auxiliar em novas pesquisas, tanto em relação as aplicações em codificação de rede, por meio dos códigos de subespaços n-shot geometricamente uniforme e do isomorfismo proposto entre o reticulado de grupo e o diagrama de Hasse de espaços projetivos, quanto em relação as aplicações em codificação de rede quântica, por meio dos códigos quânticos de subespaços na grassmanniana.

Este trabalho de doutorado apresenta contribuições em codificação no espaço projetivo, uma área de pesquisa recente que possui importantes aplicações em codificação de rede. O elo entre codificação no espaço projetivo e a codificação de rede se dá por meio do canal de comunicação matricial, onde códigos obtidos para este canal podem serem usados para evitar problemas consideráveis existentes em redes de comunicação, tais como, erros nos canais, falhas dos códigos de rede, desconhecimento da topologia da rede do canal. Especificamente, códigos no espaço projetivo podem serem modificados para códigos matriciais com aplicações em codificação de rede não-coerente. Desse modo, primeiramente, apresentamos uma definição e uma construção de códigos de subespaços n-shot geometricamente uniforme, que são códigos de bloco no espaço projetivo ou simplesmente códigos de subespaços com propriedades algébricas e geométrica interessantes, tanto do ponto de vista matemático quanto de comunicações, além de possuírem eficientes algoritmos associados ao processo de decodificação. Também apresentamos um isomorfismo entre o reticulado de um grupo abeliano consistindo do grupo das unidades do corpo finito $\mathbb{F}_p$ e o diagrama de Hasse de espaços projetivos $\mathbb{P}(\mathbb{F}_p^m)$, onde uma possibilidade é tratar códigos de subespaços n-shot nessa estrutura. E por fim, apresentamos construções de códigos quânticos de subespaços na grassmanniana, por meio do mapeamento por partição de conjuntos. A primeira descreve um estado quântico separável arbitrário universal e a partir desse mapeamento foi obtido o código quântico de subespaço na grassmanniana associado a um estado de máximo emaranhamento global. E através dessa associação obtivemos novos estados quânticos de máximo emaranhamento global. A segunda proposta, associa códigos de subespaços na grassmanniana diretamente a estados quânticos puros de máximo emaranhamento global, proveniente de uma matriz modificada dos códigos de Reed-Muller, dando origem ao código quântico de subespaço na grassmanniana, onde tais propostas, contemplam aplicações em codificação de rede quântica. Nesta linha de pesquisa, o trabalho acaba tocando, ao longo de seu conteúdo, em aspectos de diversas áreas do conhecimento como álgebra, design combinatório, teoria de códigos corretores de erros, codificação em espaço projetivo, computação quântica e informação quântica entre outras.

Recapitulando o conteúdo do trabalho, no Capítulo 1 foram apresentados, uma

breve motivação de possível aplicações de tais resultados, uma breve descrição de trabalhos anteriores, a proposta e o detalhamento do trabalho.

O Capítulo 2 foi dedicado à apresentação de conceitos para o entendimento e desenvolvimento dos principais resultados dos capítulos posteriores. No Capítulo 3 foram apresentados os primeiros resultados do nosso trabalho, onde propusemos a definição de códigos de subespaço n-shot geometricamente uniforme e uma construção de tais códigos. No Capítulo 4, fazendo parte das contribuições, apresentamos um isomorfismo entre o reticulado do grupo abeliano (grupo multiplicativo) do corpo finito $\mathbb{F}_p$ e o diagrama de Hasse de espaços projetivos $\mathbb{P}(\mathbb{F}_p^m)$.

Finalmente, o Capítulo 5 apresentamos duas propostas de rotulamentos para o tratamento de estados quânticos de máximo emaranhamento global segundo a medida de Meyer-Wallach. A primeira associa o estado quântico separavél arbitrário universal um código de subespaço na grassmanniana com a máxima distância de subespaço e a segunda, associa diretamente a estado quântico puro de máximo emaranhamento global, proveniente de uma matriz modificada dos códigos de Reed-Muller à códigos de subespaços de máxima distância de subespaço, ambas dando origem ao que chamamos de códigos quânticos de subespaços na grassmanniana.

Perspectivas de Pesquisa

Dados os resultados, há uma série de trabalhos futuros possíveis de se realizar, e listamos a seguir alguns deles.

Com respeito aos códigos de subespaços n-shot geometricamente uniformes:

- Analisar e realizar estudos sobre o conceito de códigos de subespaços n-shot geometricamente uniforme para corpos finitos $\mathbb{F}_p$, onde $p > 2$ primo.
- Analisar e realizar estudos sobre o conceito de códigos de subespaços n-shot geometricamente uniforme para outras estruturas algébricas, como exemplo, os anéis $\mathbb{Z}_q$, com q um inteiro positivo.
- Realizar estudos sobre o conceito de códigos de subespaços n-shot geometricamente uniforme para outras métricas, como as métricas da injeção e do posto.

Com respeito ao problema de isomorfismo de reticulados de grupos e espaços projetivos:

- Estudar a aplicação do isomorfismo apresentado nos códigos de subespaços n-shot.
- Realizar estudos na direção de construir isomorfismo entre reticulados associados a outras classes de grupos e diagrama de Hasse de espaços projetivos.

- Comparação da complexidade computacional requerida no projeto, codificação e decodificação de códigos de subespaços n-shot em $\mathbb{P}(\mathbb{F}_p^m)^n$ em ambas as estruturas.

Com respeito ao problema de códigos quânticos de subespaços:

- Estender as propostas de rotulamento considerando agora quaisquer código de subespaço no espaço projetivo.
- Estudar a proteção desigual em relação aos códigos associados aos subsistemas.

Referências

AHLSWEDE, R.; CAI, N.; LI, R.; YEUNG, R. Network information flow. *IEEE Transactions on Information Theory*, v. 46, p. 1204–1216, 2000.

BRAUN, M.; ETZION, T.; VARDY, A. Linearity and complements in projective space. *Linear Algebra and Its Applications*, v. 438, p. 57–70, 2013.

BRAUN, M.; KIERMAIER, M.; NAKIC, A. *On the automorphism group of a binary q-analog of the Fano plane*. [S.l.]: arxiv.org/1501.0779v1, 2016.

CALDERBANK, R. Multilevel codes and multistage decoding. IEEE Transactions on Communications, v. 37, p. 222–229, 1989.

COULBORN, C. J.; DINITZ, J. H. *Handbook of combinatorial design*. 2. ed. [S.l.]: Chapman Hall/CRC, 2007.

DOMINGUES, H. H.; IEZZI, G. *Álgebra moderna*. 4. ed. [S.l.]: Atual Editora, 2003.

ETZION, T.; RAVIV, N. Equidistant codes in the Grassmannian. Discrete Applied Mathematics, v. 186, p. 187–197, 2015.

ETZION, T.; SILBERSTEIN, N. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. IEEE Transactions on Information Theory, v. 55, n. 7, p. 2909–2919, 2009.

ETZION, T.; STORME, L. Galois geometries and coding theory. Designs, Codes and Cryptography, v. 78, p. 311–350, 2016.

ETZION, T.; VARDY, A. Error-correcting codes in projective space. IEEE Transactions on Information Theory, v. 57, p. 1165–1173, 2011.

FORNEY, G. D. Geometrically uniform codes. IEEE Transactions on Information Theory, v. 37, n. 5, p. 1241–1260, 1991.

GAZZONI, V. C. Estudo do emaranhamento quântico com base na teoria de codificação clássica. Tese de Doutorado - Programa de Pós Graduação em Engenharia Elétrica - FEEC-UNICAMP, Campinas - SP, 2008.

GREENBERGER D. M., H. M. A. S. A.; ZEILINGER, A. Bell's theorem without inequalities. Am. J. Phys., v. 58, p. 1131, 1990.

IMAI, H.; HIRAKAWA, S. A new multilevel coding method using error-correcting codes. IEEE Transactions on Information Theory, v. 23, n. 3, p. 371–377, 1977.

KHALEGHI, A.; SILVA, D.; KSCHISCHANG, F. R. Subspace codes. Lecture Notes in Computer Science, v. 5921, p. 1–21, 2009.

KöETTER, R.; KSCHISCHANG, F. R. Coding for errors and erasures in random network coding. IEEE Transactions on Information Theory, v. 54, n. 8, p. 3579–3591, 2008.

LI, R.; YEUNG, W.; CAI, N. Linear network coding. *IEEE Transactions on Information Theory*, v. 49, p. 371–381, 2003.

LIMA, L. B. *Aplicações de álgebra linear em ruídos quânticos*. [S.l.]: Dissertação de Mestrado Profissional - Programa de Pós Graduação em Matemática - IMECC-UNICAMP, Campinas - SP, 2007.

LIMA, L. B.; PALAZZO, R. Geometrically uniform n-shot subspace codes. Electronic Notes in Discrete Mathematics, v. 57, p. 47–54, 2017.

LIMA, L. B.; PALAZZO, R. Similaridade entre a estrutura algébrica associada a espaços projetivos e design combinatório via diagrama de Hasse. C.Q.D. – Revista Eletrônica Paulista de Matemática, p. 119–127, 2017.

MACWILLIAMS, F. J.; SLOANE, N. J. A. *The theory of error-correcting codes*. [S.l.]: The Mathematical Association of America, 1983. v. 21.

MIYAMOTO, G. A. Códigos de subespaço geometricamente uniformes. Dissertação de Mestrado - Programa de Pós Graduação em Engenharia Elétrica - FEEC-UNICAMP, Campinas-SP, 2015.

NIELSEN, M. A.; CHUANG, I. L. *Quantum computation and quantum information*. 1. ed. [S.l.]: Cambridge Univeristy Press, 2000.

NóBREGA, R. W. Canais matriciais multiplicativos sobre corpos e anéis finitos com aplicações em codificação de rede. *Tese de Doutorado - Programa de Pós-Graduação em Engenharia Elétrica - UFSC, Florianópolis-SC*, 2013.

NóBREGA, R. W.; UCHôA-FILHO, B. Multishot codes for network coding: bounds and a multilevel construction. IEEE Intl Symp. on Information Theory - ISIT-09, p. 428–432, 2009.

ROMAN, S. *Lattices and ordered sets*. 4. ed. [S.l.]: Springer, 2008.

ROTMAN, J. J. *An introduction to the theory of groups*. 4. ed. [S.l.]: Springer Verlag, 1993.

SILVA, D.; KSCHISCHANG, F. R.; KöETTER, R. Communication over finite-field matrix channels. IEEE Transactions on Information Theory, v. 56, n. 2, p. 1296–1305, 2010.

SLEPIAN, D. Group codes for the Gaussian channel. Bell Labs Technical Journal, v. 47, p. 575–602, 1968.

STINSON, D. R. *Combinatorial designs:constructions and analysis*. [S.l.]: Springer, 2004.

UNGERBOEK, G. Channel coding multilevel/phase signals. IEEE Transactions on Information Theory, v. 28, n. 2, p. 55–67, 1982.

YEUNG, R. W.; CAI, N. Network error correction, Part I: Basic concepts and upper bounds. Communications in Information and Systems, v. 6, n. 1, p. 19–36, 2006.