



UNIVERSIDADE ESTADUAL DE  
CAMPINAS

Instituto de Matemática, Estatística e  
Computação Científica

RODRIGO LABIAK

## **Simetrias em Geometria de Distâncias**

Campinas

2017

Rodrigo Labiak

## **Simetrias em Geometria de Distâncias**

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática .

Orientador: Fernando Eduardo Torres Orihuela

Coorientador: Carlile Campos Lavor

Este exemplar corresponde à versão final da Dissertação defendida pelo aluno Rodrigo Labiak e orientada pelo Prof. Dr. Fernando Eduardo Torres Orihuela.



Campinas

2017

**Agência(s) de fomento e nº(s) de processo(s): CAPES**

Ficha catalográfica  
Universidade Estadual de Campinas  
Biblioteca do Instituto de Matemática, Estatística e Computação Científica  
Ana Regina Machado - CRB 8/5467

L113s Labiak, Rodrigo, 1993-  
Simetrias em geometria de distâncias / Rodrigo Labiak. – Campinas, SP :  
[s.n.], 2017.

Orientador: Fernando Eduardo Torres Orihuela.

Coorientador: Carlile Campos Lavor.

Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de  
Matemática, Estatística e Computação Científica.

1. Simetria (Matemática). 2. Reflexão parcial (Simetria). 3. Geometria de  
distâncias. I. Torres Orihuela, Fernando Eduardo, 1961-. II. Lavor, Carlile  
Campos, 1968-. III. Universidade Estadual de Campinas. Instituto de  
Matemática, Estatística e Computação Científica. IV. Título.

Informações para Biblioteca Digital

**Título em outro idioma:** Symmetries in distance geometry

**Palavras-chave em inglês:**

Symmetry (Mathematics)

Partial reflection (Symmetry)

Distance geometry

**Área de concentração:** Matemática

**Titulação:** Mestre em Matemática

**Banca examinadora:**

Fernando Eduardo Torres Orihuela [Orientador]

Dessislava Hristova Kochloukova

Giuliano Gadioli La Guardia

**Data de defesa:** 20-02-2017

**Programa de Pós-Graduação:** Matemática

**Dissertação de Mestrado defendida em 20 de fevereiro de 2017 e aprovada**

**Pela Banca Examinadora composta pelos Profs. Drs.**

**Prof.(a). Dr(a). FERNANDO EDUARDO TORRES ORIHUELA**

**Prof.(a). Dr(a). DESSISLAVA HRISTOVA KOCHLOUKOVA**

**Prof.(a). Dr(a). GIULIANO GADIOLI LA GUARDIA**

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

*Aos meus pais...*

# Agradecimentos

Agradeço inicialmente a Deus, por ter sido meu refúgio seguro nos momentos de angústia e incertezas.

Aos professores Carlile Campos Lavor e Fernando Eduardo Torres Orihuela por terem me orientado neste trabalho e por todas as oportunidades que me proporcionaram durante esses dois anos.

Aos professores Giuliano Gadioli La Guardia e Dessislava Hristova Kochloukova por participar da banca de avaliação. Em especial ao professor Giuliano Gadioli La Guardia pelo incentivo e orientação durante a graduação.

À toda minha família pelo apoio, que mesmo com a distância se fez presente em todos os momentos. Em especial à minha mãe, meu pai, meu irmão, minhas avós e meus avôs.

Aos amigos do Imecc, especialmente Robert, Sergio e Carlos por toda a ajuda nos estudos, pelo companheirismo e pelos bons momentos que proporcionaram durante estes dois anos.

Aos amigos de Moradia, Marilene, João, Lucas, Wildiner, Bruno, Marcos e Mateus pela amizade e pelos bons momentos que proporcionaram durante minha estadia na G4A.

Aos amigos que ficaram no Paraná, Juliana, Rodrigo, Danilo, Diego, Ana Cláudia, Josiane e Amanda, pela amizade, pelas conversas e pelo apoio.

À CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior cujo apoio financeiro tornou possível a realização deste trabalho.

# Resumo

O problema principal de Geometria de Distâncias (GD) é determinar as posições de um conjunto de pontos, considerando conhecidas algumas distâncias. Este trabalho tem como principal objetivo estudar uma classe particular de problemas da GD, onde aparecem simetrias que podem ajudar a caracterizar todas as soluções do problema. Apresentamos os resultados para o  $\mathbb{R}^3$ , os quais podem ser generalizados para o  $\mathbb{R}^n$ .

**Palavras-chave:** Simetrias, Operadores de Reflexão, Geometria de Distâncias.

# Abstract

The main problem of Distance Geometry (GD) is to determine the positions of a set of points, considering some known distances. This work has as main objective to study a particular class of problems of DG, where there are symmetries that can be used to characterize all the solutions of the problem. We present the results for  $\mathbb{R}^3$ , which can be also generalized to  $\mathbb{R}^n$ .

**Keywords:** Symmetries, Reflection Operators, Distance Geometry.



# Lista de ilustrações

Figura 1	– Na figura à esquerda, a ilustração da Definição 3.1, e na figura à direita, a ilustração da Definição 3.2. . . . .	23
Figura 2	– No caso (a), observa-se a não simetria para o caso $\lambda(\eta) = \lambda(\beta) = 1$ . No caso (b), observa-se a simetria quando temos $\lambda(\eta) = 1 - \lambda(\beta)$ . . . . .	26
Figura 3	– Ilustração do fato de que $a_u \cdot a_v^0 = a_u \cdot a_v^1$ , apresentado na demonstração do Teorema 3.1. . . . .	26
Figura 4	– Ilustração da Proposição 3.2 em $\mathbb{R}^2$ . . . . .	28
Figura 5	– Na figura à esquerda, a ilustração para o caso em que temos somente um subnó. Na figura à direita, a ilustração para o caso em que temos dois subnós. . . . .	29
Figura 6	– Ilustração do contra-exemplo 4.2 para $K = 2$ . Note que os nós $x_5^{(00)}, x_5^{(01)}, x_5^{(11)}$ são factíveis. Entretanto, o nó $x_5^{(10)}$ não satisfaz $d_{1,5}$ . . . . .	39
Figura 7	– Um contra-exemplo para o Lema 3.1 quando aplicado em $PDGD_3 \setminus PDGDM$ , também para $K = 2$ . . . . .	39
Figura 8	– Ilustração da Proposição 5.2 com $K = 2$ , $d_{ut}$ com cardinalidade 2 e $d_{uv}$ sendo um único valor. . . . .	46
Figura 9	– Ilustração da utilização de distância intervalar para realizar podas na árvore de busca. . . . .	54

# Sumário

	<b>Introdução</b> . . . . .	<b>11</b>
<b>1</b>	<b>O PROBLEMA DE GEOMETRIA DE DISTÂNCIAS</b> . . . . .	<b>12</b>
1.1	Interseções de $n$ Esferas no $\mathbb{R}^n$ e Reflexões no $\mathbb{R}^n$ . . . . .	12
1.2	Conceitos e Resultados sobre a Teoria de Grupos . . . . .	13
<b>2</b>	<b>ALGORITMO BP</b> . . . . .	<b>15</b>
2.1	O PDGDM . . . . .	15
2.2	Ramificação e Poda . . . . .	16
2.3	A Árvore de Busca do BP . . . . .	18
<b>3</b>	<b>GEOMETRIA NA ÁRVORE DO BP</b> . . . . .	<b>22</b>
3.1	Operadores de Reflexão Parcial e Probabilidade de Eventos Condi- cionais . . . . .	22
3.2	Reflexões na árvore BP . . . . .	24
<b>4</b>	<b>SIMETRIA E O NÚMERO DE SOLUÇÕES</b> . . . . .	<b>32</b>
4.1	Relação com sequências binárias e o Grupo de Reflexões Parciais . . . . .	32
4.2	Cardinalidade do Conjunto de Soluções . . . . .	37
4.3	Contra-exemplos . . . . .	38
<b>5</b>	<b>O ALGORITMO IBP</b> . . . . .	<b>41</b>
5.1	Nova Ordem nos Vértices . . . . .	41
5.2	Algoritmo iBP . . . . .	42
5.2.1	Geometria na Árvore do iBP . . . . .	44
5.3	O Número de Soluções . . . . .	48
5.3.1	Poda por Intervalos . . . . .	53
<b>6</b>	<b>CONSIDERAÇÕES FINAIS</b> . . . . .	<b>55</b>
	<b>REFERÊNCIAS</b> . . . . .	<b>56</b>

# Introdução

O problema principal da Geometria de Distâncias é determinar as posições de um conjunto de pontos, considerando conhecidas apenas algumas distâncias entre estes (CRIPPEN; HAVEL, 1988). Neste trabalho, apresentamos os resultados para o espaço  $\mathbb{R}^3$  e fornecemos exemplos e ilustrações no  $\mathbb{R}^2$  para facilitar a visualização e compreensão dos resultados apresentados nesta dissertação.

Nosso principal objetivo é estudar simetrias no Problema Discretizável de Geometria de Distâncias Moleculares (PDGDM). Além de sua importância teórica, este problema está relacionado ao cálculo da estrutura 3D de moléculas de proteínas que utiliza dados de experimentos de Ressonância Magnética Nuclear (RMN) que, por sua vez, estão associados a distâncias entre átomos próximos da molécula. As simetrias do PDGDM podem acelerar a resolução do problema através do método Branch and Prune (BP) (LIBERTI et al., 2014b), (LIBERT; LAVOR; MUCHERINO, 2013), (LAVOR; LIBERTI; MUCHERINO, 2013).

Outro objetivo é determinar a cardinalidade do conjunto solução do PDGDM, que está associado às simetrias mencionadas acima.

Por fim, consideramos uma versão mais geral do PDGDM, em que algumas distâncias podem não ser mais representadas por valores exatos. Essa extensão do PDGDM é importante, pois vários problemas reais associados, com destaque para o cálculo de estrutura molecular, apresentam incertezas nos valores das distâncias.

# 1 O Problema de Geometria de Distâncias

Iniciamos com a definição formal do problema principal da Geometria de Distâncias.

**Definição 1.1.** (*LIBERTI et al., 2014a*). *Problema de Geometria de Distâncias (PGD).* Dado um inteiro positivo  $K$  e um grafo simples ponderado e não direcionado  $G = (V, E, d)$ , onde  $d : E \rightarrow \mathbb{R}_+$ , encontre uma função  $x : V \rightarrow \mathbb{R}^K$  tal que

$$\forall \{u, v\} \in E \quad \|x_u - x_v\| = d_{uv}. \quad (1.1)$$

Uma função  $x : V \rightarrow \mathbb{R}^K$  é dita uma realização. Dizemos que uma realização é válida se esta satisfaz a Equação (1.1). Uma questão importante a ser tratada é o custo computacional para se obter uma solução.

Agora, definiremos uma versão "discreta" do problema, onde o espaço de busca é finito.

**Definição 1.2.** (*LIBERTI et al., 2014a*). *Problema Discretizável de Geometria de Distâncias (PDGD<sub>3</sub>):* Considere um grafo  $G = (V, E, d)$  de um PGD, com  $K = 3$  e uma ordem em  $V$ , denotada por  $v_1, \dots, v_n$ , tal que:

- existe uma realização válida para  $v_1, v_2, v_3$ ,
- para todo  $v_i$ ,  $i = 4, \dots, n$ , existem no mínimo três vértices antecessores  $a_i, b_i, c_i$  com  $\{\{a_i, v_i\}, \{b_i, v_i\}, \{c_i, v_i\}\} \subseteq E$  satisfazendo

$$d_{a_i b_i} + d_{b_i c_i} > d_{a_i c_i}.$$

Encontre uma função  $x : V \rightarrow \mathbb{R}^3$  tal que

$$\forall \{v_i, v_j\} \in E, \quad \|x_{v_i} - x_{v_j}\| = d_{v_i v_j}.$$

Como veremos no próximo capítulo, existe um algoritmo, denominado Branch-and-Prune (BP), que resolve o PDGD<sub>3</sub> explorando o espaço de busca do problema, representado por uma árvore binária. A principal operação do BP é calcular interseção de esferas.

## 1.1 Interseções de $n$ Esferas no $\mathbb{R}^n$ e Reflexões no $\mathbb{R}^n$

Nesta seção, apresentamos as observações necessárias sobre reflexões e esferas no  $\mathbb{R}^n$ . As observações a seguir são argumentos importantes para o desenvolvimento do trabalho.

**Observação 1.1.** (COOPE, 2000). Sejam  $a_1, \dots, a_n \in \mathbb{R}^n$  os centros de  $n$  esferas de raios dados por  $d_1, \dots, d_n$  respectivamente. Se os pontos  $a_1, \dots, a_n$  não estão todos contidos em nenhum hiperplano de  $\mathbb{R}^n$ , então a interseção das  $n$  esferas gera, no máximo, dois pontos.

**Observação 1.2.** (BRADY; WATT, 2006). Se  $a$  é um vetor unitário em  $\mathbb{R}^K$ ,  $H$  representa um hiperplano contendo a origem e normal a  $a$ , então o operador de reflexão  $R_0$ , em relação à  $H$ , tem representação matricial dada por

$$[R_0] = I - 2[a][a]^\top,$$

onde  $I$  é a matriz identidade  $K \times K$  e  $[a]$  é a matriz  $K \times 1$  cujas entradas são as coordenadas de  $a$ . Em outras palavras, as reflexões com respeito a hiperplanos são isometrias que podem ser representadas por operadores lineares.

Seja  $H$  um hiperplano com equação  $a^\top x = a_0$ , em que  $a_0 \neq 0$ , e seja  $a_i$ , para algum  $1 \leq i \leq K$ , o coeficiente não nulo de menor índice em  $a$ . Então, o operador reflexão  $R$  que age sobre um ponto  $p \in \mathbb{R}^K$ , com respeito à  $H$ , é dado por

$$R(p) = R_0(p - \frac{a_0}{a_i} e_i) + \frac{a_0}{a_i} e_i,$$

onde  $e_i \in \mathbb{R}^K$  é o vetor unitário com 1 no índice  $i$  e 0 nos demais, ou seja, primeiro transladamos  $p$  para que possamos fazer a reflexão usando o operador  $R_0$  com respeito à translação de  $H$  contendo a origem, e depois realiza-se a translação inversa da reflexão obtida.

## 1.2 Conceitos e Resultados sobre a Teoria de Grupos

Para estudar as simetrias envolvidas nas versões discretas do PDG, utilizaremos a Teoria de Grupos. Listamos abaixo os principais conceitos e resultados necessários para o desenvolvimento deste trabalho.

**Definição 1.3.** Um conjunto não vazio de elementos  $G$  é dito ser um **grupo** se em  $G$  está definida uma operação binária, chamada de produto e denotada por  $\cdot$ , tal que

- $a, b \in G$  implica que  $a \cdot b \in G$  (fechamento);
- $a, b, c \in G$  implica que  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  (propriedade associativa);
- Existe um elemento  $e \in G$  tal que  $a \cdot e = e \cdot a = a$  para todo  $a \in G$  (existência de um elemento identidade em  $G$ );
- Para cada  $a \in G$  existe um elemento  $a^{-1} \in G$  tal que  $a \cdot a^{-1} = a^{-1} \cdot a = e$  (existência de inversos em  $G$ ).

**Definição 1.4.** Um grupo  $G$  é dito ser abeliano ou comutativo se para cada  $a, b \in G$ ,  $a \cdot b = b \cdot a$ .

**Definição 1.5.** Um subconjunto não vazio  $H$  de um grupo  $G$  é dito ser um **subgrupo** de  $G$  se, sob o produto em  $G$ ,  $H$  é também um grupo.

**Lema 1.1.** Um subconjunto  $H$  do grupo  $G$  é um subgrupo de  $G$  se, e somente se,

1.  $a, b \in H$  implica que  $a \cdot b \in H$ .

2.  $a \in H$  implica que  $a^{-1} \in H$ .

*Demonstração.* Ver ([HERSTEIN, 1975](#)) ou ([GARCIA; LEQUAIN, 2008](#)). □

**Definição 1.6.** Sejam  $(G, \cdot)$  e  $(H, \times)$  dois grupos. Uma aplicação  $f : G \rightarrow H$  é um **homomorfismo** se ela é compatível com as estruturas dos grupos, isto é,

$$f(a \cdot b) = f(a) \times f(b), \quad \forall a, b \in G.$$

**Definição 1.7.** Um homomorfismo  $f$  de  $G$  para  $H$  é dito ser um **isomorfismo** se  $f$  é bijetora.

**Definição 1.8.** Dois grupos  $G$  e  $H$  são ditos **isomorfos** se existe um isomorfismo de  $G$  para  $H$ . Escrevemos  $G \cong H$ .

**Definição 1.9.** Sejam  $G$  um grupo,  $C$  um conjunto e  $\mathcal{P}(C)$  o grupo de permutações de  $C$ . Uma representação de  $G$  no grupo de permutações de  $C$  é um homomorfismo  $f : G \rightarrow \mathcal{P}(C)$ . Diz-se também que o grupo  $G$  age sobre o conjunto  $C$ .

## 2 Algoritmo BP

Neste capítulo, vamos apresentar uma versão do Algoritmo BP um pouco diferente da versão original apresentada em (LIBERTI; LAVOR; MACULAN, 2008).

Nas Seções 2.1 e 2.2, apresentamos uma nova versão da Definição 1.2, restrita a uma classe de instâncias, algumas observações e resultados importantes sobre a ordem dos vértices.

Na Seção 2.3, descrevemos o Algoritmo BP.

### 2.1 O PDGDM

O Problema Discretizável de Geometria de Distâncias Moleculares (*PDGDM*) é um subconjunto de instâncias do *PDGD*<sub>3</sub> e sua generalização para uma dimensão  $K$  arbitrária é denotada por  ${}^K PDGDM$  (LIBERTI et al., 2014a). Entretanto, neste trabalho, vamos nos restringir ao caso em que  $K = 3$ , com ilustrações dos resultados e definições para  $K = 2$ . A diferença entre o *PDGDM* e o *PDGD*<sub>3</sub> é que os vértices utilizados no *PDGDM* para calcular a posição de um vértice  $v$  são antecessores imediatos de  $v$ .

Considere um conjunto  $U = \{x_i \in \mathbb{R}^3 | i \leq 4\}$  de pontos em  $\mathbb{R}^3$ . Sejam  $n = |V|$  e  $m = |E|$  e  $N(v) = \{u \in V | \{u, v\} \in E\}$  para todo  $v \in V$ , o conjunto de vértices adjacentes à  $v$ . Para uma ordem  $<$  sobre  $V$ , seja  $\gamma(v) = \{u \in V | u < v\}$  o conjunto dos antecessores de  $v$  e seja  $\rho(v) = |\gamma(v)| + 1$  a posição de  $v$  nesta ordem. Dado  $V' \subset V$ , denotamos por  $G[V']$  o subgrafo de  $G$  induzido por  $V'$ . Dado um conjunto finito  $M$ , seja  $\mathcal{P}(M)$  seu conjunto de partes. Dada uma sequência  $x = (x_1, \dots, x_n)$  e um subconjunto  $U \subset \{1, \dots, n\}$ , seja  $x[U]$  a subsequência de  $x$  indexada por  $U$ . Se  $x$  é uma subsequência inicial de  $y$ , então  $y$  é uma extensão de  $x$ . Para  $U_v = \{v - 3, v - 2, v - 1\}$ , seja  $\bar{x}$  a realização de  $G[U_v]$ .

**Definição 2.1. Problema Discretizável de Geometria de Distâncias Moleculares (*PDGDM*):** Considere um grafo  $G = (V, E, d)$  de um *PGD* com  $K = 3$  e uma ordem em  $V$  denotada por  $v_1, \dots, v_n$  tal que:

1. Existe uma realização válida para  $v_1, v_2, v_3$ ;
2. Para todo  $v_i$ ,  $i = 4, \dots, n$ , existem, pelo menos 3 vértices imediatamente anteriores  $v_{i-3}, v_{i-2}, v_{i-1}$ , em que  $\{v_{i-3}, v_{i-2}, v_{i-1}, v_i\}$  é uma clique e

$$d_{v_{i-3}v_{i-2}} + d_{v_{i-2}v_{i-1}} > d_{v_{i-3}v_{i-1}}.$$

Encontre uma função  $x : V \rightarrow \mathbb{R}^3$  tal que

$$\forall \{v_i, v_j\} \in E, \|x_{v_i} - x_{v_j}\| = d_{v_i v_j}. \quad (2.1)$$

A Condição 1 exclui realizações obtidas via rotações e translações. A Condição 2 exige os vértices de nenhuma 3-clique determinados por antecessores imediatos sejam realizados colinearmente.

## 2.2 Ramificação e Poda

Consideremos um instância  $PDGDM$ . Seja  $v \in V$  com nível  $\rho(v) > 3$ ,  $G^v = G[\gamma(v) \cup \{v\}]$  e  $x$  uma realização válida de  $G[\gamma(v)]$ . Nos próximos resultados, estamos interessados no número de extensões válidas para a realização de  $G^v$ .

**Lema 2.1.** *Se  $|N(v) \cap \gamma(v)| = 3$ , então existem no máximo duas extensões distintas de  $x$  que são válidas para  $G^v$ . Além disso, se existe uma extensão válida, então, com probabilidade 1, existem exatamente duas extensões válidas.*

*Demonstração.* Por hipótese,  $|N(v) \cap \gamma(v)| = 3$ . Assim,  $U_v = N(v) \cap \gamma(v) = \{v-3, v-2, v-1\}$  e  $v$  pertence à interseção de exatamente 3 esferas em  $\mathbb{R}^3$ , onde cada esfera tem centro  $x_u$ , raio  $d_{uv}$ ,  $u \in U_v$ . A posição  $z \in \mathbb{R}^3$  de  $v$  deve então satisfazer:

$$\begin{aligned} \forall u \in U_v, \quad \|z - x_u\| = d_{uv} &\Rightarrow \|z - x_u\|^2 = d_{uv}^2 \\ &\Rightarrow \langle z - x_u, z - x_u \rangle = d_{uv}^2 \\ &\Rightarrow \langle z, z \rangle - 2\langle z, x_u \rangle + \langle x_u, x_u \rangle = d_{uv}^2 \\ &\Rightarrow \|z\|^2 - 2x_u \cdot z + \|x_u\|^2 = d_{uv}^2. \end{aligned} \quad (2.2)$$

Considerando  $v-1 \in U_v$  e subtraindo a linha indexada por  $v-1$  da equação (2.2) das outras linhas de 2.2, obtemos o sistema:

$$\begin{cases} 2(x_{v-2} - x_{v-1}) \cdot z = (\|x_{v-2}\|^2 - d_{v-2v}^2) - (\|x_{v-1}\|^2 - d_{v-1v}^2) \\ 2(x_{v-3} - x_{v-1}) \cdot z = (\|x_{v-3}\|^2 - d_{v-3v}^2) - (\|x_{v-1}\|^2 - d_{v-1v}^2) \\ \|z\|^2 - 2x_{v-1} \cdot z + \|x_{v-1}\|^2 = d_{v-1v}^2. \end{cases} \quad (2.3)$$

Note que o sistema (2.3) é composto por 2 equações lineares e uma única equação quadrática no 3-vetor  $z$ . Escrevemos as equações lineares como um sistema  $Az = b$ , onde

$$A = \begin{bmatrix} 2(x_{v-2} - x_{v-1}) \\ 2(x_{v-3} - x_{v-1}) \end{bmatrix}, \quad b = \begin{bmatrix} (\|x_{v-2}\|^2 - d_{v-2v}^2) - (\|x_{v-1}\|^2 - d_{v-1v}^2) \\ (\|x_{v-3}\|^2 - d_{v-3v}^2) - (\|x_{v-1}\|^2 - d_{v-1v}^2) \end{bmatrix}.$$

A matriz  $A$  tem dimensão  $2 \times 3$  e  $b \in \mathbb{R}^2$ . Vamos supor que a matriz  $A$  não tem posto completo. Então, pela condição de dependência linear,

$$\xi_{v-2}(x_{v-2} - x_{v-1}) + \xi_{v-3}(x_{v-3} - x_{v-1}) = 0,$$

para alguns coeficientes  $\xi_{v-2}, \xi_{v-3} \neq 0$ , o que implica que  $x_{v-3}$  pertence ao espaço gerado de  $\{x_{v-2}, x_{v-1}\}$ , ou seja,  $x_{v-3}, x_{v-2}, x_{v-1}$  são colineares, o que contradiz a hipótese



da desigualdade triangular estrita. Logo,  $A$  tem posto completo. Assim, sem perda de generalidade, assuma que a matriz quadrada  $B$  formada pelas primeiras duas colunas de  $A$  seja invertível. Seja  $z_B$  o vetor consistindo das primeiras duas componentes de  $z$ . Então, pela parte linear do sistema (2.3), temos:

$$Bz_B = b - Nz_3,$$

onde  $N = \begin{bmatrix} 2(x_{v-2,3} - x_{v-1,3}) \\ 2(x_{v-3,3} - x_{v-1,3}) \end{bmatrix}$ , resultando em  $z_B = B^{-1}(b - Nz_3)$  como uma função  $z_B(z_3)$  de  $z_3$ . Substituindo  $z_B$  no sistema (2.3) como  $z_B(z_k)$ , obtemos:

$$\begin{aligned} d_{v-1,v}^2 &= \| B^{-1}(b - Nz_3) \|^2 + z_3^2 - 2x_{v-1,B}(B^{-1}(b - Nz_3)) - 2x_{v-1,3}z_3 + \| x_{v-1,B} \|^2 \\ &\quad + x_{v-1,3}^2 \\ &= \| B^{-1}b - B^{-1}Nz_3 \|^2 + z_3^2 - 2x_{v-1,B}B^{-1}b + 2x_{v-1,B}B^{-1}Nz_3 - 2x_{v-1,3}z_3 \\ &\quad + \| x_{v-1,B} \|^2 + x_{v-1,3}^2. \end{aligned}$$

Fazendo  $\bar{b} = B^{-1}b$  e  $\bar{N} = B^{-1}N$ , temos:

$$\begin{aligned} d_{v-1,v}^2 &= \| \bar{b} - \bar{N}z_3 \|^2 + z_3^2 - 2x_{v-1,B}\bar{b} + 2x_{v-1,B}\bar{N}z_3 - 2x_{v-1,3}z_3 + \| x_{v-1,B} \|^2 + x_{v-1,3}^2 \\ &= \| \bar{b} \|^2 - 2\langle \bar{b}, \bar{N}z_3 \rangle + \| \bar{N}z_3 \|^2 + z_3^2 - 2x_{v-1,B}\bar{b} + 2x_{v-1,B}\bar{N}z_3 - 2x_{v-1,3}z_3 \\ &\quad + \| x_{v-1,B} \|^2 + x_{v-1,3}^2 \\ &= (\| \bar{N} \|^2 + 1)z_3^2 + \langle \bar{b}, \bar{b} \rangle + \langle x_{v-1,B}, x_{v-1,B} \rangle - 2\langle x_{v-1,B}, \bar{b} \rangle \\ &\quad - 2((\bar{b} - x_{v-1,B})\bar{N} + x_{v-1,3})z_3 + x_{v-1,3}^2. \end{aligned}$$

Obtemos, então, a seguinte equação quadrática na variável  $z_3$ :

$$(\| \bar{N} \|^2 + 1)z_3^2 + \| x_{v-1,B} - \bar{b} \|^2 - 2((\bar{b} - x_{v-1,B})\bar{N} + x_{v-1,3})z_3 + x_{v-1,3}^2 - d_{v-1,v}^2 = 0 \quad (2.4)$$

Se o discriminante da Equação (2.4) é negativo, então não existe extensão válida de  $\bar{x}$  para  $v$  e o resultado segue. Se o discriminante é não negativo, temos soluções  $z'_3, z''_3$ , gerando os pontos  $z' = (z_B(z'_3), z'_3)$ ,  $z'' = (z_B(z''_3), z''_3) \in \mathbb{R}^3$ , que são distintos com probabilidade 1, pois o discriminante 0 tem probabilidade 0. As realizações estendidas, distintas com probabilidade 1, são dadas por  $(x, z')$  e  $(x, z'')$ .  $\square$

Geometricamente, o Lema 2.1 pode ser visto como a interseção de 3 esferas no  $\mathbb{R}^3$ , o que gera um conjunto solução com no máximo dois pontos.

**Lema 2.2.** *Se  $|N(v) \cap \gamma(v)| > 3$ , então, com probabilidade 1, existe no máximo uma extensão de  $x$ .*

*Demonstração.* Consideremos um subconjunto  $S \subseteq N(v) \cap \gamma(v)$ , tal que  $|S| = 4$  e  $S \supseteq U_v$ . Assim, existe pelo menos um ponto  $x_v$  tal que  $(x, x_v)$  é uma realização de  $G[S \cup \{v\}]$ , em relação ao sistema

$$\forall u \in S, \quad x_{v,1}^2 - 2x_{u,1}x_{v,1} + x_{u,1}^2 + x_{v,2}^2 - 2x_{u,2}x_{v,2} + x_{u,2}^2 + x_{v,3}^2 - 2x_{u,3}x_{v,3} + x_{u,3}^2 = d_{uv}^2 \quad (2.5)$$

ou o sistema não tem solução. No último caso, o resultado segue. Assuma agora que existe um ponto  $x_v$  satisfazendo o sistema (2.5). Como os pontos  $x_u$  são conhecidos,  $\forall u \in S$ , observe que o sistema (2.5) é um sistema quadrático com 3 variáveis e 4 equações. Assim, como na demonstração do Lema 2.1, obtemos um sistema linear equivalente ao sistema (2.5). Com probabilidade 1, os pontos  $\{x_u | u \in S\}$  são não coplanares, implicando que o sistema associado tenha exatamente uma solução, como queríamos demonstrar.  $\square$

Geometricamente, o Lema 2.2 pode também ser visto como a interseção de 4 esferas no  $\mathbb{R}^3$ , o que gera um conjunto solução com no máximo um ponto.

**Lema 2.3.** *Utilizando a notação do Lema 2.1, se  $\bar{x}$  é uma realização para  $G[U_v]$ , então  $z''$  é uma reflexão de  $z'$ , com respeito ao plano dado pelos 3 pontos de  $\bar{x}$ .*

*Demonstração.* As duas soluções encontradas no Lema 2.1, pertencem a interseção de 3 esferas em  $\mathbb{R}^3$ . Como qualquer esfera em  $\mathbb{R}^3$  é simétrica com respeito a qualquer plano passando por seu centro. Implica que a interseção de até 3 esferas em  $\mathbb{R}^3$  é simétrica com respeito ao plano contendo todos os centros das 3 esferas. Assim, os pontos  $z, z'$  são reflexões entre si.  $\square$

## 2.3 A Árvore de Busca do BP

Denotaremos a árvore de busca binária BP por  $\mathcal{T} = (\mathcal{V}, \mathcal{A})$ , em que  $\mathcal{V}$  é o conjunto de nós e  $\mathcal{A}$  é o conjunto dos caminhos entre os nós. Os caminhos que conectam o nó raiz aos nós folhas são representados por trincas  $\alpha = (x(\alpha), \lambda(\alpha), \mu(\alpha))$ , onde  $p(\alpha)$  é o único caminho do nó raiz de  $\mathcal{T}$  até  $\alpha$  e  $\alpha^-$  são os únicos nós antecessores de  $\alpha$ , exceto quando  $\alpha = r$  (nó raiz). Neste caso, definimos  $r^- = r$ . O símbolo  $x(\alpha)$  é definido recursivamente para denotar uma extensão da realização  $x^- = x(\alpha^-)$  encontrada sobre  $p(\alpha^-)$ . O símbolo  $\lambda(\alpha) \in \{0, 1\}$  descreve se  $\alpha$  é um subnó à "direita" ou à "esquerda" do plano gerado por  $\alpha^-$ . Especificamente, dado um nó  $\alpha$  no nível  $i$  em  $\mathcal{T}$ ,  $v = \rho^{-1}(i)$ , seja  $\bar{x}$  uma realização parcial de  $G[U_v]$  e  $a_v^\top x = a_{v0}$  a equação do plano mediante dos pontos de  $\bar{x}$ . Assumindo que  $u = \rho^{-1}(i-1)$  e  $a_v \in \mathbb{R}^3$  é orientado quando  $a_v a_u \geq 0$  então:

$$\lambda(\alpha) = \begin{cases} 0 & \text{se } a_v^\top x(\alpha)_i \leq a_{v0} \\ 1 & \text{se } a_v^\top x(\alpha)_i > a_{v0} \end{cases} \quad (2.6)$$

Dizemos que  $\mu(\alpha) = \boxplus$ , se  $x(\alpha)$  é uma extensão válida de  $x^-$  (neste caso o nó é dito ser factível) e  $\mu(\alpha) = \boxminus$  caso contrário. Deste modo, podemos encontrar todo o conjunto de

realizações válidas  $X$  de  $G$  simplesmente analisando  $\mathcal{T}$  a partir dos nós folhas marcados por  $\boxplus$  até chegar ao nó raiz  $r$ .

---

**Algoritmo 1** O algoritmo BP
 

---

**Exige:** Realização parcial  $\bar{x}$  dos 3 primeiros vértices de  $G$

**Obtém:** O conjunto  $X$  de realizações de  $G$

- 1: Sejam  $\alpha = (\bar{x}_1, 0, \boxplus)$  e  $\alpha' = (\bar{x}_1, 1, \boxminus)$
- 2: Iniciar  $\mathcal{V} = \{\alpha, \alpha'\}$  e  $\mathcal{A} = \{(r, \alpha), (r, \alpha')\}$
- 3: **para**  $1 < i \leq 3$  **fazer**
- 4:   Sejam  $\alpha = (\bar{x}_i, 0, \boxplus)$ ,  $\alpha' = (\bar{x}_i, 1, \boxminus)$ ,  $\beta = (\bar{x}_{i-1}, 0, \boxplus)$
- 5:   Sejam  $\mathcal{V} \leftarrow \mathcal{V} \cup \{\alpha, \alpha'\}$  e  $\mathcal{A} \leftarrow \mathcal{A} \cup \{(\beta, \alpha), (\beta, \alpha')\}$
- 6: **fim para**
- 7:   *BranchAndPrune*(4,  $(\bar{x}_3, 0, \boxplus)$ )
- 8: Seja  $X = \{x(\theta) | \theta \in \mathcal{V} \wedge |N^+(\theta)| = 0 \wedge \mu(\theta) = \boxplus\}$
- 9: **parar**
- 10:
- 11: **função** *BranchAndPrune*( $i, \beta$ )
- 12: **se**  $i > n \vee \mu = \boxminus$  **então**
- 13:   **retornar**
- 14: **fim se**
- 15: Seja  $v = \rho^{-1}(i)$
- 16: Calcular a equação  $a_v^\top x = a_{v0}$  do plano através de  $x[U_v]$
- 17: Sejam  $Z = \{z', z''\}$  as extensões de  $x(\beta)$  para  $v$ , e  $Z' = Z$
- 18: **para**  $z \in Z$  **fazer**
- 19:   **se**  $\exists \{u, v\} \in E \parallel x(\beta)_u - z \parallel \neq d_{uv}$  **então**
- 20:     Seja  $Z = Z - \{z\}$
- 21:   **fim se**
- 22: **fim para**
- 23: **se**  $Z = \{z', z''\}$  **então**
- 24:   **se**  $a_v^\top z' \leq a_{v0}$  **então**
- 25:     Sejam  $\alpha = (z', 0, \boxplus)$ ,  $\alpha' = (z'', 1, \boxplus)$
- 26:   **senão**
- 27:     Sejam  $\alpha = (z'', 0, \boxplus)$ ,  $\alpha' = (z', 1, \boxplus)$
- 28:   **fim se**
- 29: **senão se**  $Z = \{z\}$  **então**
- 30:   **if**  $a_v^\top z = a_{v0}$  **então**
- 31:     Sejam  $\alpha = (z, 0, \boxplus)$ ,  $\alpha' = (Z' - \{z\}, 1, \boxminus)$
- 32:   **senão**

---

```

33:     Sejam  $\alpha = (z, 1, \boxplus)$ ,  $\alpha' = (Z' - \{z\}, 0, \boxminus)$ 
34:   fim se
35: senão
36:   retornar
37: fim se
38: Sejam  $\mathcal{V} \leftarrow \mathcal{V} \cup \{\alpha, \alpha'\}$  e  $\mathcal{A} \leftarrow \mathcal{A} \cup \{(\beta, \alpha), (\beta, \alpha')\}$ 
39: para  $\theta \in N^+(\beta)$  tal que  $\mu(\theta) = \boxplus$  fazer
40:    $BranchAndPrune(i + 1, \theta)$ 
41: fim para
42: retornar

```

---

Agora, faremos uma breve explicação do funcionamento do Algoritmo BP.

Inicialmente, é fornecido ao algoritmo a realização  $\bar{x}_1$  do primeiro vértice e define-se  $\alpha = (\bar{x}_1, 0, \boxplus)$  e  $\alpha' = (\bar{x}_1, 1, \boxminus)$ . Então, define-se o conjunto dos nós  $\mathcal{V} = \{\alpha, \alpha'\}$  e o conjunto dos caminhos  $\mathcal{A} = \{(r, \alpha), (r, \alpha')\}$ . Para um vértice  $i$  na ordem, tal que  $1 < i \leq 3$ , é definido  $\alpha = (\bar{x}_i, 0, \boxplus)$ ,  $\alpha' = (\bar{x}_i, 1, \boxminus)$  e  $\beta = (\bar{x}_{i-1}, 0, \boxplus)$ . Isto é, fixa-se uma realização para os 3 primeiros vértices da ordem e atualiza-se os conjuntos dos nós e dos caminhos tomando-se  $\mathcal{V} \leftarrow \mathcal{V} \cup \{\alpha, \alpha'\}$  e  $\mathcal{A} \leftarrow \mathcal{A} \cup \{(\beta, \alpha), (\beta, \alpha')\}$ . Em seguida, utiliza-se o método BP para encontrar as possíveis realizações para o vértice 4, estendendo a realização da 3-clique inicial. Além disso, define-se o conjunto solução  $X$  dado pelas realizações  $x(\theta)$ , tal que  $\theta \in \mathcal{V}$ ,  $|N^+(\theta)| = 0$ , isto é, a cardinalidade dos vértices seguintes na ordem é zero, e o símbolo  $\mu(\theta) = \boxplus$ , ou seja,  $x(\theta)$  é uma extensão válida de  $x(\theta^-)$ .

Para o próximo passo, utiliza-se o método de busca BP para encontrar todos os nós possíveis para o nível  $i$  e, estendendo a realização do nó  $\beta$  determinado anteriormente, estabelece-se a condição de retorno dada por  $i > n \vee \mu = \boxminus$  ou seja, chegar ao elemento final da ordem ou encontrar um nó não factível.

Tomando  $v = \rho^{-1}(i)$ , calcula-se a equação do plano  $a_v^\top x = a_{v0}$  através dos pontos de  $x[U_v]$ . Considera-se o conjunto  $Z = \{z', z''\}$  dos nós que são extensão de  $x(\beta)$  para o  $v$ , além disso define-se  $Z = Z'$ . Para cada  $z \in Z$ , se existir uma aresta de poda  $\{u, v\} \in E$ , tal que  $\|x(\beta)_u - z\| \neq d_{uv}$ , então este nó é excluído do conjunto  $Z$ . No caso em que  $Z = \{z', z''\}$ . Se  $a_v^\top z' \leq a_{v0}$ , implica  $\alpha = (z', 0, \boxplus)$  e  $\alpha' = (z'', 1, \boxplus)$ . Entretanto, se  $a_v^\top z' \geq a_{v0}$ , implica  $\alpha = (z', 1, \boxplus)$  e  $\alpha' = (z'', 0, \boxplus)$ . No caso em que  $Z = \{z\}$ . Se  $a_v^\top z \leq a_{v0}$ , implica  $\alpha = (z, 0, \boxplus)$  e  $\alpha' = (Z' - \{z\}, 1, \boxminus)$ . Entretanto, se  $a_v^\top z \geq a_{v0}$ , implica  $\alpha = (z, 1, \boxplus)$  e  $\alpha' = (Z' - \{z\}, 0, \boxminus)$ . Para o caso em que  $Z$  é o conjunto vazio, retorna-se para o próximo nó em  $\rho^{-1}(i)$ .

Em seguida, atualiza-se o conjunto de nós e o conjunto de caminhos tomando  $\mathcal{V} \leftarrow \mathcal{V} \cup \{\alpha, \alpha'\}$  e  $\mathcal{A} \leftarrow \{(\beta, \alpha), (\beta, \alpha')\}$ , respectivamente. Para  $\theta \in N^+(\beta)$  tal que  $\mu(\theta) = \boxplus$ ,

utiliza-se o método BP para o vértice  $i + 1$  e retorna-se para verificação da condição de retorno no passo 12.

**Lema 2.4.** *Ao término da execução do Algoritmo BP,  $X$  contém todas as realizações válidas de  $G$  estendidas de  $\bar{x}$ .*

*Demonstração.* Pelo Lema 2.1, temos que  $Z$ , no passo 17, existe com probabilidade 1. Cada realização em  $X$  é válida devido aos passos 17, 19 e 20. Além disso, pelos Lemas 2.1 e 2.2, não existe outra extensão válida de  $\bar{x}$ .  $\square$

As realizações encontradas são incongruentes, exceto pelas reflexões existentes dos planos definidos por  $\bar{x}_1, \dots, \bar{x}_v$ , onde  $\bar{x}_i$  é conjunto de nós que são realizações dos vértices antecessores imediatos do vértice  $i$ . O número dessas reflexões é determinado pela ordem em  $V$  e pelas arestas em  $E$ .

A seguir, provaremos que nenhum nível de  $\mathcal{T}$  possui dois nós factíveis, com um e dois subnós factíveis, respectivamente, considere uma partição de  $\mathcal{V}$  em subconjuntos disjuntos dois a dois,  $\mathcal{V}_1, \dots, \mathcal{V}_n$ , onde para todo  $i \leq n$ , o conjunto  $\mathcal{V}_i$  contém todos os nós de  $\mathcal{V}$  pertencente ao nível  $i$  da árvore  $\mathcal{T}$ .

**Proposição 2.1.** *Com probabilidade 1, não existe um nível  $i \leq n$  possuindo dois nós realizáveis distintos  $\beta, \theta \in \mathcal{V}_i$ , tais que  $|\{\alpha \in N^+(\beta) | \mu(\alpha) = \boxplus\}| = 1$  e  $|\{\alpha \in N^+(\theta) | \mu(\alpha) = \boxplus\}| = 2$ .*

*Demonstração.* Demonstraremos que para todo  $i \leq n$ , o evento onde dois nós distintos  $\beta, \theta \in \mathcal{V}_i$ , com  $\rho^{-1}(i) = v$ , tal que  $\beta$  tem somente um subnó factível e  $\theta$  possui dois subnós factíveis, tem probabilidade 0 de ocorrer. Considere  $T_v = N(v) \cap \gamma(v)$ ; se  $|T_v| = 3$ , então pelo Lema 2.1, com probabilidade 1,  $\beta$  possui exatamente dois subnós factíveis. Contudo, por hipótese, ele possui somente um, assim, o evento  $|T_v| = 3$  ocorre com probabilidade 0. Já que  $|T_v| \geq 3$  pela Condição 2 da Definição 2.1, o evento  $|T_v| > 3$  ocorre com probabilidade 1. Pelo Lema 2.2, existe, com probabilidade 1, no máximo uma realização válida estendendo a realização parcial em  $v$ , implicando que os dois subnós de  $\theta$  representam a mesma realização cujo evento ocorre com probabilidade 0.  $\square$

**Observação 2.1.** *Note que para  $l \in \{i, \dots, n\}$  e  $\forall \alpha \in \mathcal{V}_l$ , o conjunto  $p(\alpha) \cap \mathcal{V}_i$  possui um único elemento, sendo este elemento o nó pertencente ao nível  $i$  sobre o caminho  $\alpha$  até o nó raiz da árvore do BP.*

### 3 Geometria na Árvore do BP

Neste capítulo, demonstramos que dada uma realização válida  $y \in X$ , onde no nível  $i = \rho(v)$ , a árvore do BP possui dois ramos que continuam até o último nível, então a realização obtida refletindo todos os pontos de  $y$ , após o  $(i - 1)$ -ésimo vértice, através do plano definido pelos nós pertencentes a  $y$  que são realizações dos vértices em  $U_v$  é, com probabilidade 1, válida. Denotamos por  $y[U_v]$  o conjunto de nós pertencentes a  $y$  que são realizações dos vértices em  $U_v$ .

Na Seção 3.1, estabelecemos uma condição suficiente para que uma instância seja realizável e, no mínimo, um nó apresente dois subnós factíveis. A seguir, construímos um operador de reflexão parcial que representa a ação de uma reflexão em determinado nível de uma realização  $y \in X$  e demonstramos algumas propriedades deste operador.

Na Seção 3.2, mostramos diversos resultados sobre reflexões parciais das realizações.

#### 3.1 Operadores de Reflexão Parcial e Probabilidade de Eventos Condicionais

**Definição 3.1.** *Seja  $y \in X$  e  $v \in V - \{v_1, v_2, v_3\}$  denotamos por  $\Upsilon(y, v)$  a seguinte propriedade: Existem nós folhas factíveis  $\beta, \beta' \in \mathcal{V}_n$  tais que  $x(\beta) = y$ ,  $p(\beta) \cap \mathcal{V}_{\rho(v)-1} = p(\beta') \cap \mathcal{V}_{\rho(v)-1}$  e  $p(\beta) \cap \mathcal{V}_{\rho(v)} \neq p(\beta') \cap \mathcal{V}_{\rho(v)}$ .*

**Definição 3.2.** *Considerando  $\Upsilon(y, v)$  válida e  $\mathbb{R}^v$  o operador de reflexão com respeito ao plano através de  $y[U_v]$ , definimos:*

$$\tilde{R}^v = I^{\rho(v)-1} \times (R^v)^{n-\rho(v)}.$$

*Em outras palavras,  $\tilde{R}^v y = (y_1, \dots, y_{\rho(v)-1}, R^v y_{\rho(v)}, \dots, R^v y_n)$ , para qualquer  $y$ .*

Observamos que esta é uma reflexão parcial de  $y$  que age somente sobre os vértices de nível maior que  $\rho(v) - 1$ . Veja as ilustrações das Definições 3.1 e 3.2 para dimensão  $K = 2$  na Figura 1

Note que a matriz que representa  $R^v$  depende da realização  $y \in X$ . Entretanto, estamos interessados em fazer com que  $R^v$  represente a ação de uma reflexão no nível  $v$ , ao invés da própria matriz de reflexão. Para isto, considere uma relação sobre o conjunto de todas as possíveis realizações  $V \rightarrow \mathbb{R}^3$ , não necessariamente válidas, estendendo  $\bar{x}$ . Seja  $E_d \subseteq E$  o conjunto de arestas  $\{u, v\} \in E$  tal que  $|\rho(v) - \rho(u)| \leq 3$  e  $G_d$  o subgrafo de  $G$

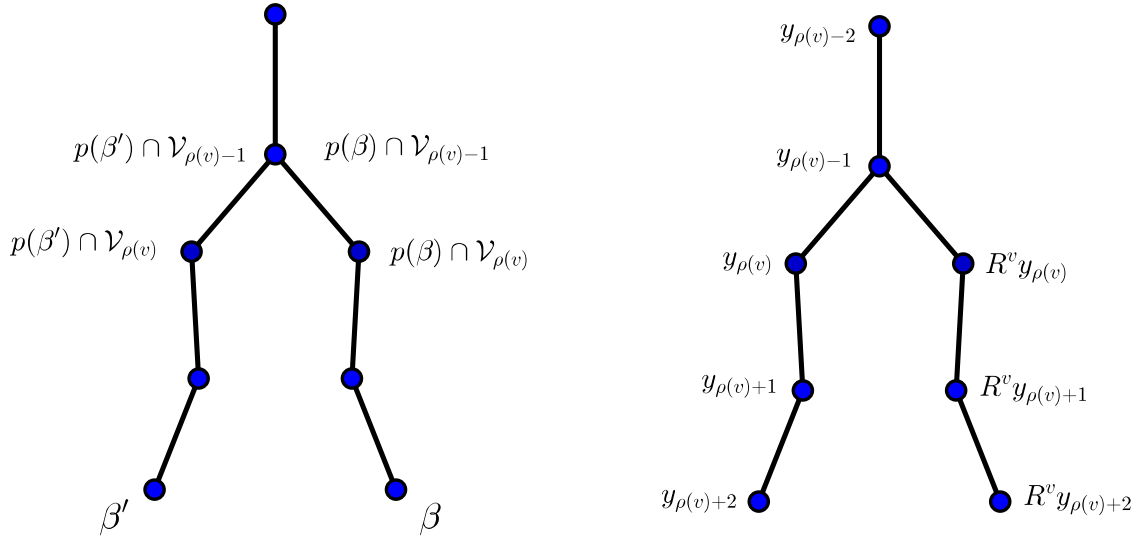


Figura 1 – Na figura à esquerda, a ilustração da Definição 3.1, e na figura à direita, a ilustração da Definição 3.2.

definido por  $E_d$ . Dizemos que duas realizações  $y, y'$  estão relacionadas se ambas são válidas para  $G_d$ .

**Proposição 3.1.** *A relação  $S$ , dada por  $ySy'$  se, e somente se,  $y$  e  $y'$  são realizações válidas para  $G_d$ , é uma relação de equivalência.*

*Demonstração.* Sejam  $y, y', y''$  realizações de  $V \rightarrow \mathbb{R}^3$  não necessariamente válidas estendendo  $\bar{x}$ . Claramente  $S$  é reflexiva, pois se  $y$  é uma realização válida para  $G_d$ , então  $ySy$ . Mostraremos que  $S$  é simétrica: se  $ySy'$ , então  $y$  e  $y'$  são ambas realizações válidas para  $G_d$ , implicando que  $y'Sy$ . Por fim, mostraremos que  $S$  é transitiva: se  $ySy'$  e  $y'Sy''$ , então  $y, y', y''$  são realizações válidas para  $G_d$ , e assim,  $ySy''$ . Portanto,  $S$  é uma relação de equivalência.  $\square$

Agora, podemos definir  $R^v$  como sendo o conjunto de matrizes de reflexão no nível  $\rho(v)$  sobre todas as realizações da mesma classe de equivalência. Além disso, esta definição é também herdada por  $\tilde{R}^v$ .

O próximo resultado garante que, dados dois subnós factíveis de um mesmo nó factível, ambos estão associados a realizações parciais cujas últimas componentes são  $K$ -vetores, os quais são reflexões entre si através do plano dado pelos 3 nós antecessores imediatos.

**Corolário 3.1.** *Seja  $\alpha \in \mathcal{V}_{i-1}$ , para algum  $i > 1$ ,  $v = \rho^{-1}(i)$  e  $N^+(\alpha) = \{\eta, \beta\}$ , com  $\mu(\eta) = \mu(\beta) = \boxplus$ . Então,  $x(\eta)_v = R^v x(\beta)_v$ .*

*Demonstração.* Pelo Lema 2.3, temos que as respectivas realizações  $x(\eta)$  e  $x(\beta)$  são reflexões entre si com relação ao plano definido por  $U_v$ , implicando que cada nó no nível  $j, j > i$ , de  $x(\eta)$  é reflexão do nó no nível  $j$  de  $x(\beta)$  com relação ao plano definido por  $U_v$ . Portanto,  $x(\eta)_v = R^v x(\beta)_v$ .  $\square$

Nos próximos resultados deste capítulo, vamos assumir que as instâncias PDGDM são instâncias realizáveis, fazendo com que as probabilidades sejam condicionais. A seguir, apresentamos uma observação sobre a relação entre a propriedade  $\Upsilon(y, v)$  e a condição de uma instância ser realizável.

**Observação 3.1.** *Se  $\Upsilon(y, v)$  é válida para algum  $y \in X$  e  $v \in V - \{v_1, v_2, v_3\}$ , então, pela definição, existem nós folhas realizáveis na árvore do BP, o que implica que a instância PDGDM é realizável.*

Uma consequência direta da observação acima é que assumir a propriedade  $\Upsilon(y, v)$  ser válida e afirmar um resultado com probabilidade 1 é equivalente a assumir que a probabilidade condicional para o evento ocorrer em uma instância PDGDM realizável é 1. Assim, temos que alguns pontos realizados estão à distâncias conhecidas, pois caso contrário, a instância não seria realizável, ou seja, as distâncias entre os pontos não satisfazem as Equações (1.1).

O sentido das afirmações, nos próximos resultados, que para certos escalares reais e vetores pertencem a certos conjuntos com probabilidade 1 é que a Medida de Probabilidade de Lebesgue das instâncias realizáveis que não satisfazem o resultado é nula no conjunto de todas as instâncias realizáveis.

## 3.2 Reflexões na árvore BP

Iniciaremos esta seção com um resultado técnico que vai nos indicar o valor de  $\lambda$  na trinca referente à realização do nó.

**Lema 3.1.** *Seja  $\alpha \in \mathcal{V}_{i-1}$  para algum  $i > 1$ , tal que  $N^+(\alpha) = \{\eta', \beta'\}$ ,  $u = \rho^{-1}(i)$ ,  $v$  com  $\rho(v) = l$ , tal que  $l \geq i$ , e considere dois nós factíveis  $\eta, \beta \in \mathcal{V}_l$ , tais que  $\{\eta'\} = p(\eta) \cap \mathcal{V}_i$  e  $\{\beta'\} = p(\beta) \cap \mathcal{V}_i$ . Além disso,  $\forall i \leq j \leq l$ , seja  $w = \rho^{-1}(j)$ ,  $p(\eta) \cap \mathcal{V}_j = \{\eta''\}$  e  $p(\beta) \cap \mathcal{V}_j = \{\beta''\}$ . Então, com probabilidade 1, as seguintes condições são equivalentes:*

1.  $\forall i \leq j \leq l, \quad x(\beta'')_w = R^u x(\eta'')_w;$
2.  $\forall i \leq j \leq l, \quad \lambda(\eta'') = 1 - \lambda(\beta'').$

*Demonstração.* Sejam  $a_v^{0\top} x = a_{v0}^0$ ,  $a_v^{1\top} x = a_{v0}^1$  as equações dos planos  $H_\eta, H_\beta$ , respectivamente, definidos por  $x(\eta)[U_v]$  e  $x(\beta)[U_v]$ , com vetores normais orientados como descrito



na Observação 1.2. Vamos demonstrar por indução sobre  $l$  que a seguinte condição é equivalente a (1) e (2):

3.  $\forall i \leq j \leq l$ ,  $x(\beta'')_w = R^u x(\eta'')_w$  e  $a_u \cdot a_w^0 = a_u \cdot a_w^1$ , onde  $a_w^0$  e  $a_w^1$  são os vetores normais dos planos  $H_{\eta''}$  e  $H_{\beta''}$  orientados usualmente.

Para  $l = i$ , temos que (1) e (3) valem simultaneamente. De fato, temos que  $\eta = \eta'$  e  $\beta = \beta'$ , e pelo Corolário 3.1,  $x(\beta)_v = R^u x(\eta)_v$ , e do Algoritmo BP, passos 25 e 27, obtemos que  $\lambda(\eta) = 1 - \lambda(\beta)$ . Além disso, temos  $H_\eta = R^u H_\beta$ . Assim,  $|a_u \cdot a_v^0| = |a_u \cdot a_v^1|$  e como a orientação de  $a_v^0$ ,  $a_v^1$  é tal que  $a_u \cdot a_v^0, a_u \cdot a_v^1 \geq 0$ , o resultado é válido para  $l = i$ . Assumindo por hipótese de indução que as equivalências são válidas para o nível  $l - 1$ , mostraremos que isto implica o resultado ser válido para o nível  $l$ . De agora em diante, denote  $t = \rho^{-1}(l - 1)$

(3)  $\Rightarrow$  (1) É óbvio.

Vejam os (1)  $\Rightarrow$  (2). Suponhamos que  $\forall i \leq j < l$ ,  $x(\beta'')_w = R^u x(\eta'')_w$  e  $\lambda(\eta'') = 1 - \lambda(\beta'')$ . Pela hipótese de indução, as duas igualdades são equivalentes. Daí, temos que os 3 pontos que geram os planos  $H_{\eta''}$  e  $H_{\beta''}$  pertencem a  $H_\alpha$  ou são reflexões entre si por  $H_\alpha$  e, portanto,  $H_{\eta''} = R^u H_{\beta''}$  é válida para todo  $j$ . Em particular, é verdade se escolhermos  $\eta'', \beta'' \in \mathcal{V}_{l-1}$ . Ainda pela hipótese de indução, de (1)  $\Rightarrow$  (3), temos que  $a_u \cdot a_t^0 = a_u \cdot a_t^1$ . Logo,  $a_t^0, a_t^1$  tem direção semelhante com relação a  $a_u$ . Portanto,  $\lambda(\eta) = 1 - \lambda(\beta)$  se, somente se,  $x(\beta)_v = R^u x(\eta)_v$ .

Vejam os (2)  $\Rightarrow$  (3). Suponhamos que  $\forall i \leq j \leq l$ ,  $\lambda(\eta'') = 1 - \lambda(\beta'')$ . Demonstramos na implicação anterior que  $\forall i \leq j \leq l$ ,  $x(\beta'')_w = R^u x(\eta'')_w$ . Resta demonstrar que  $a_u \cdot a_v^0 = a_u \cdot a_v^1$ , isto é, que o ângulo  $\theta_v^0$  e  $\theta_v^1$  formado por esses vetores tem o mesmo cosseno. Observamos novamente que  $H_\eta = R^u H_\beta$ . Pela hipótese de indução, sabemos que os ângulos  $\theta_t^0, \theta_t^1$  formados por  $a_u$  e por  $a_t^0, a_t^1$ , respectivamente, possuem o mesmo cosseno. Com probabilidade 1, os planos  $H_\eta, H_\beta$  não são paralelos, assim seus vetores normais não são idênticos. Portanto  $\theta_t^0 = -\theta_t^1$  (veja a ilustração na Figura 3). Denotamos por  $\theta^0, \theta^1$ , os ângulos formados por  $a_t^0$  e  $a_v^0$  e por  $a_t^1$  e  $a_v^1$ , respectivamente. Também temos que  $H_{\eta''} = R^u H_{\beta''}$ , onde  $\eta'', \beta'' \in \mathcal{V}_{l-1}$ . Consequentemente, os vetores normais desses quatro planos são simétricos, o que implica que  $\theta^0 = -\theta^1$  ou  $\theta^0 = \pi - \theta^1$ . Pela definição de  $a_v^0$  e  $a_v^1$ , como os produtos escalares são positivos, temos  $-\frac{\pi}{2} \leq \theta^0, \theta^1 \leq \frac{\pi}{2}$ , implicando que,  $\theta^0 = -\theta^1$ . Portanto,  $\theta_v^0 = \theta_t^0 + \theta^0 = -\theta_t^1 - \theta^1 = -\theta_v^1$  e  $\cos \theta_v^0 = \cos(-\theta_v^1) = \cos \theta_v^1$ .  $\square$

No caso em que  $K = 2$ , a Figura 2 representa o fato de que os itens (i) e (ii) do Lema 3.1 são equivalentes.

A próxima proposição estabelece que, considerando vértices  $u, v \in V$ , tais que  $|\rho(v) - \rho(u)| = 4$ , e  $y$  sendo uma realização válida, então existem somente dois valores reais positivos de  $\|y_u - y_v\|$ .

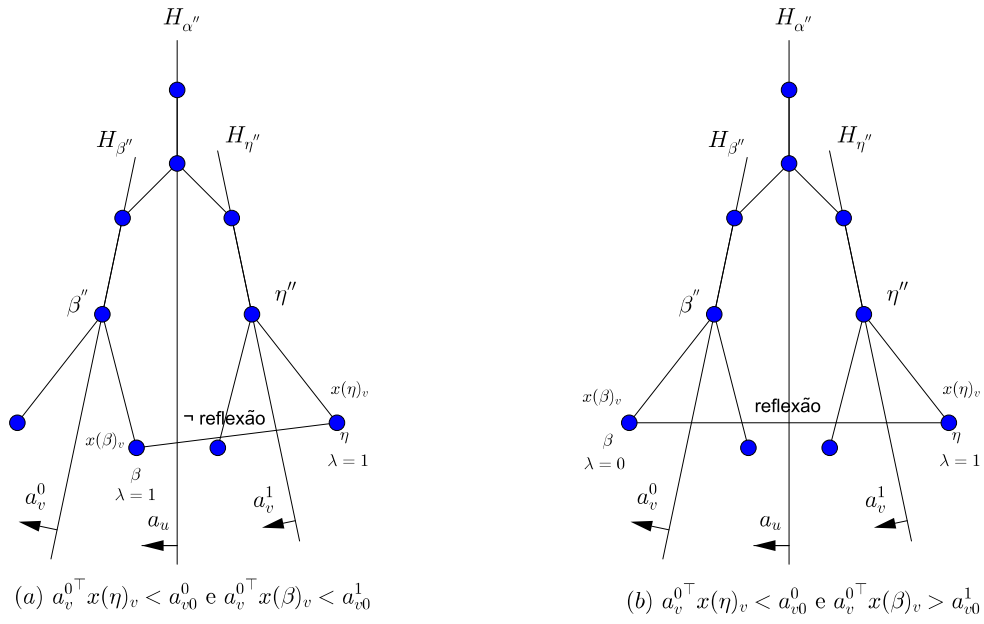


Figura 2 – No caso (a), observa-se a não simetria para o caso  $\lambda(\eta) = \lambda(\beta) = 1$ . No caso (b), observa-se a simetria quando temos  $\lambda(\eta) = 1 - \lambda(\beta)$ .

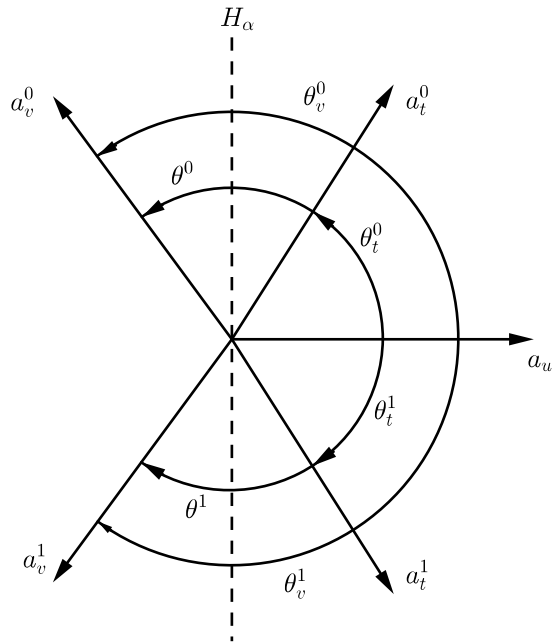


Figura 3 – Ilustração do fato de que  $a_u \cdot a_v^0 = a_u \cdot a_v^1$ , apresentado na demonstração do Teorema 3.1.

**Proposição 3.2.** *Considere uma árvore  $\mathcal{T}'$  de  $\mathcal{T}$ , consistindo de 5 níveis consecutivos  $i - 4, \dots, i$ , onde  $i \geq 7$ , enraizados em um único nó  $\eta$  e tal que todos os nós de todos os níveis são marcados por  $\boxplus$ . Seja  $p = 2^4$  e considere o conjunto  $Y' = \{y^j | j \leq p\}$  de uma realização parcial de  $G$  nos nós folhas  $\{\alpha_j | j \leq p\}$  de  $\mathcal{T}'$ , tal que, para todo  $j \leq p$ ,  $y^j = x(\alpha_j)$ . Sejam  $u = \rho^{-1}(i - 4)$  e  $v = \rho^{-1}(i)$ . Então, com probabilidade 1, existem dois positivos reais distintos  $r, r'$ , tais que  $\|y_u^j - y_v^j\| \in \{r, r'\} = H^{uv}$ , para todo  $j \leq p$ .*

*Demonstração.* Nesta demonstração, utilizaremos um pequeno abuso de notação. Para um vértice  $w \in V$ , denotamos por  $R^w$  o conjunto de todas as reflexões no nível  $w$ . Ordenando os nós  $\alpha_j$  e os correspondentes  $y^j$ , a ação de  $R^v$  sobre  $(\alpha_1, \dots, \alpha_p)$  é a permutação dada por:

$$\prod_{j \bmod 2=1} (j, j+1).$$

Seja  $t = \rho^{-1}(i - 1)$ . Como todos os nós são factíveis,  $\|y_v^j - y_t^j\| = d_{vt}$  e  $\|y_u^j - y_t^j\| = d_{ut}$ , para todo  $j \leq p$ . Note que, pela definição do PDGDM, temos que  $\{v, t\}, \{u, t\} \in E$ . Com probabilidade 1, os segmentos através de  $y_u^j$  e  $y_t^j$ , onde  $j \leq p = 2^4$ , respectivamente, não se encontram contidos nos planos que definem as reflexões  $R^v$ ; o mesmo acontece com os segmentos através de  $y_t^j$  e  $y_v^j$ . Assim, existe um conjunto  $Q$  de números reais positivos  $r_1, \dots, r_p$ , para todo  $j \leq p$ , com  $j \bmod 2 = 1$ . Temos, então,  $\|y_u^j - y_v^j\| = r_j$  e  $\|y_u^{j+1} - y_v^{j+1}\| = r_{j+1}$ , o que mostra que  $|Q| \leq p = 2^4$ . Pelo Lema 3.1, a ação de  $R^{t_1}$  sobre  $(\alpha_1, \dots, \alpha_p)$  é a permutação dada por:

$$\prod_{j \bmod 4=1} (j, j+3)(j+1, j+2).$$

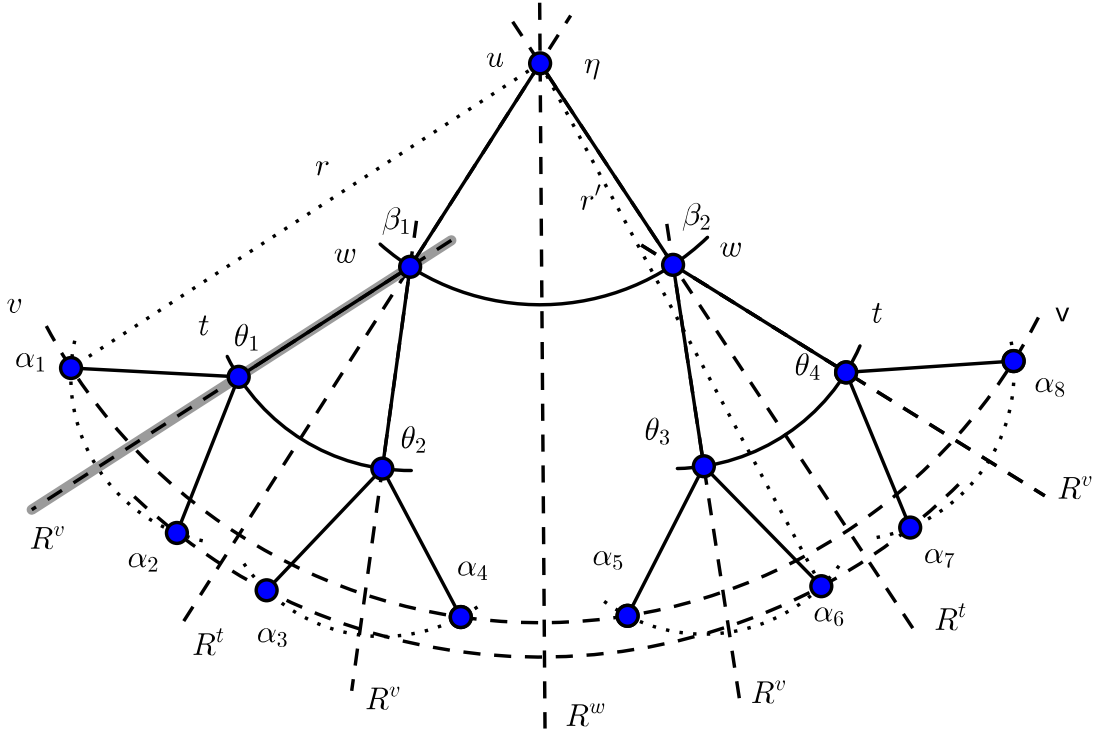
Desta forma, temos que  $r_j = r_{j+3}$  e  $r_{j+1} = r_{j+2}$ , para todo  $j \bmod 4 = 1$ . Assim, obtemos que  $|Q| \leq \frac{p}{2} = 2^3$ . Seja  $t_2 = \rho^{-1}(i - 2)$ . Pelo Lema 3.1, a ação de  $R^{t_2}$  sobre  $(\alpha_1, \dots, \alpha_p)$  é a permutação dada por:

$$\prod_{j \bmod 8=1} (j, j+7)(j+1, j+6)(j+2, j+5)(j+3, j+4).$$

Desta forma, temos  $r_j = r_{j+7}, r_{j+1} = r_{j+6}, r_{j+2} = r_{j+5}$  e  $r_{j+3} = r_{j+4}$ , para todo  $j \bmod 8 = 1$ . Assim, obtemos  $|Q| \leq \frac{p}{4} = 2^2$ . Seja  $t_3 = \rho^{-1}(i - 3)$ . Pelo Lema 3.1, a ação de  $R^{t_3}$  sobre  $(\alpha_1, \dots, \alpha_p)$  é a permutação dada por:

$$\prod_{j \bmod 16=1} (j, j+15) \dots (j+7, j+8).$$

Assim, temos  $r_j = r_{j+15}, \dots, r_{j+7} = r_{j+8}$ , para todo  $j \bmod 16 = 1$ . Daí, segue que  $|Q| \leq \frac{p}{8} = 2$ . O caso  $|Q| = 1$  ocorre somente se  $y_u^j, y_v^j, y_t^j$  são colineares, para todo  $j \leq p$ , um evento que ocorre com probabilidade 0, o que conclui a demonstração.  $\square$

Figura 4 – Ilustração da Proposição 3.2 em  $\mathbb{R}^2$ .

Observe na Figura 4, a ilustração da Proposição 3.2 para o caso em que  $K = 2$ . A disposição dos 3 segmentos dados gera, em geral, duas distâncias  $r, r'$  entre os nós folhas e o nó raiz.

No próximo resultado, apresentamos uma generalização para a Proposição 3.2, onde consideramos vértices  $u, v \in V$  com diferença de níveis arbitrária.

**Corolário 3.2.** *Considere uma subárvore  $\mathcal{T}'$  de  $\mathcal{T}$ , consistindo de  $4 + h$  níveis consecutivos  $i - h - 3, \dots, i$ , onde  $i \geq h + 6$  e  $h \geq 1$ , enraizados em um único nó  $\eta$ , tal que todos os nós de todos os níveis sejam marcados por  $\boxplus$ . Seja  $p = 2^{h+3}$  e considere o conjunto  $Y' = \{y^j | j \leq p\}$  de realizações parciais de  $G$  nos nós folhas de  $\mathcal{T}'$ . Sejam  $u = \rho^{-1}(i - h - 3)$  e  $v = \rho^{-1}(i)$ . Então, com probabilidade 1, existe um conjunto  $H^{uv} = \{r_j | j \leq 2^h\}$  de  $2^h$  reais positivos distintos, tais que  $\|y_u^j - y_v^j\| \in H^{uv}$ , para todo  $j \leq p$ .*

*Demonstração.* Para demonstrar este resultado utilizaremos indução sobre  $h$ . Para  $h = 1$ , temos pela Proposição 3.2 que o resultado é válido. Suponhamos o resultado válido para  $h = n$ , ou seja, supomos que para toda árvore  $\mathcal{T}'$  de  $\mathcal{T}$ , consistindo de  $n + 4$  níveis consecutivos, onde  $i = n + 6$  enraizados em um único nó  $\eta$ , tal que, todos os nós em todos os níveis são marcados por  $\boxplus$ . Seja  $p = 2^{n+3}$  e o conjunto  $Y' = \{y^j | j \leq p\}$  de realizações parciais de  $G$  nos nós folhas de  $\mathcal{T}'$ . Sejam  $u = \rho^{-1}(i - n - 3)$  e  $v = \rho^{-1}(i)$ . Então, com probabilidade 1, existe um conjunto  $H^{uv} = \{r_j | j \leq 2^n\}$  de  $2^n$  reais positivos distintos, tais que  $\|y_u^j - y_v^j\| \in H^{uv}$ , para todo  $j \leq p$ . Vamos provar que o resultado é válido para

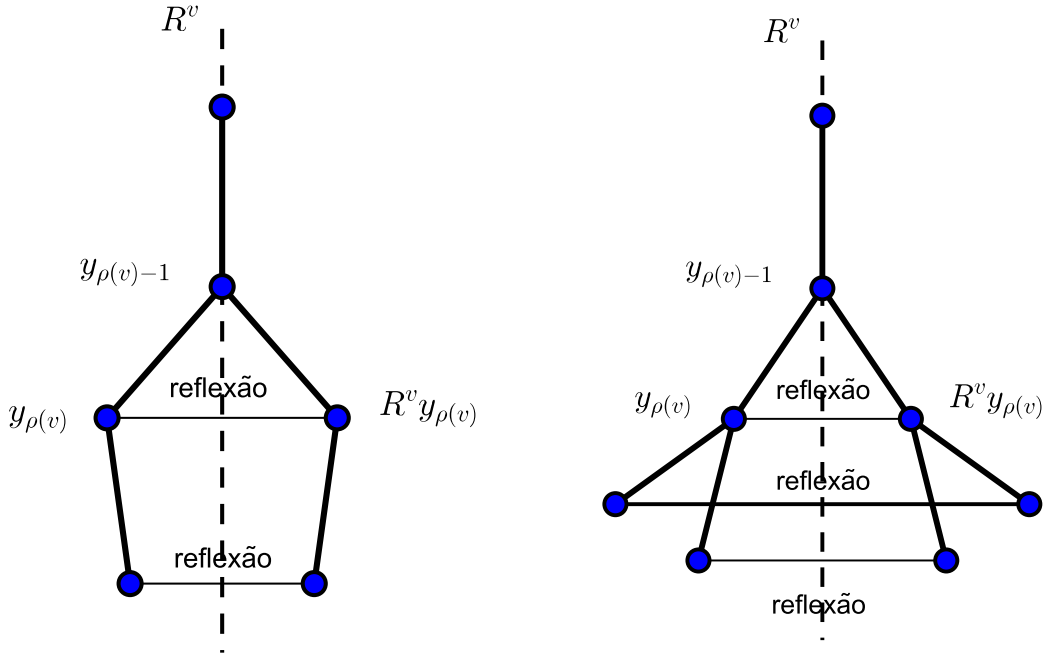


Figura 5 – Na figura à esquerda, a ilustração para o caso em que temos somente um subnó. Na figura à direita, a ilustração para o caso em que temos dois subnós.

$h = n + 1$ . Pela hipótese de indução, temos que para  $u = \rho^{-1}(i - n - 4)$  e  $v' = \rho^{-1}(i - 1)$ , com probabilidade 1, existe um conjunto  $H^{uv'} = \{r_j | j \leq 2^n\}$  de  $2^n$  reais positivos distintos tais que  $\|y_u^j - y_{v'}^j\| \in H^{uv'} \forall j \leq p$ . Além disso, pela hipótese de ser uma instância *PDGDM* realizável, cada ramo possui, no máximo, duas possibilidades para o nó folha marcado por  $\boxplus$ . Também, se um dado nó  $y^{j_1}$  é reflexão parcial por  $R^w$  de outro nó  $y^{j_2}$ , então seus subnós são reflexões entre si pela reflexão parcial  $R^w$  (veja a ilustração para a dimensão 2 na Figura 5). Assim, com probabilidade 1, dados  $u = \rho^{-1}(i - h - 3)$  e  $v = \rho^{-1}(i)$ , existe um conjunto  $H^{uv} = \{r_j | j \leq 2^{n+1}\}$  de  $2^{n+1}$  reais positivos distintos, tais que  $\|y_u^j - y_v^j\| \in H^{uv}$  para todo  $j \leq 2^{n+1}$ , o que conclui a demonstração.  $\square$

O próximo resultado mostra que, se  $\{u, v\}$  é uma aresta de  $E$  com diferença de nível maior do que 3, a distância  $d_{uv}$  pertence a um certo conjunto finito de valores sempre que a instância for unicamente realizável.

**Corolário 3.3.** *Sejam  $y \in X$  e  $v \in V - \{v_1, v_2, v_3\}$ , tal que  $\Upsilon(y, v)$  é válida. Se  $\{u, w\} \in E$ , com  $u < v < w$  e  $\rho(w) - \rho(u) > 3$ , então, com probabilidade 1,  $d_{uw} \in H^{uw}$ .*

*Demonstração.* Como  $\Upsilon(y, v)$  é válida, então a instância *PDGDM* é realizável e deve existir, pelo menos, dois nós factíveis no nível  $\rho(w)$  em  $\mathcal{T}$ . Pela interseção de 3 esferas, em  $\mathbb{R}^3$ , encontramos 2 pontos. Se  $d_{uw} \notin H^{uw}$ , a probabilidade de uma quarta esfera, em  $\mathbb{R}^3$ , conter os dois pontos é zero. Pelo Lema 2.2, a instância é unicamente realizável. Entretanto, como a instância é realizável, a distância  $d_{uw}$  não faz com que o algoritmo BP pode todas

as possíveis possibilidades. Segue, pelo Corolário 3.2, que  $d_{uw} \in H^{uw}$ , com probabilidade 1.  $\square$

No próximo resultado, vamos verificar que as reflexões dos pontos de uma realização gera pontos pertencentes a reflexão parcial de toda a realização.

**Corolário 3.4.** *Seja  $y \in X$  e  $v \in V - \{v_1, v_2, v_3\}$ , com  $\Upsilon(y, v)$  válida. Se  $u \in V$  com  $u > v$ , então  $R^v y_u$  pertence a uma extensão válida de  $y[U_v]$ .*

*Demonstração.* No caso em que não existe nenhuma aresta  $\{w, u\} \in E$ , com  $\rho(u) - \rho(w) > 3$ , o resultado segue pelo Corolário 3.1 e pelo argumento de que se um nó é reflexão de outro por alguma reflexão parcial, então os subnós destes nós também serão reflexões entre si (veja a ilustração para o caso de dimensão 2 na Figura 5). Nos demais casos, pelo Corolário 3.3, temos que  $d_{wu} \in H^{wu}$ . Como na demonstração da Proposição 3.2, todos os pares de pontos que são factíveis, em relação a  $d_{wu}$ , são reflexões um do outro com respeito a  $R^v$ .  $\square$

A seguir, vamos apresentar o principal resultado deste capítulo. Basicamente, o Teorema 3.1 afirma que, assumindo que a propriedade  $\Upsilon(y, v)$  seja válida, a reflexão parcial da realização  $y$  com respeito a um vértice  $v$  é válida. A parte mais interessante é que, assumindo novamente que  $\Upsilon(y, v)$  é válida, somente um dos ramos em  $v$  faz parte da realização de  $y$ , enquanto o outro pertence a outra realização válida distinta da mesma instância.

**Teorema 3.1.** *Seja  $y \in X$  e  $v \in V - \{v_1, v_2, v_3\}$ , tal que  $\Upsilon(y, v)$  é válida. Então, com probabilidade 1,  $\tilde{R}^v y \in X$ .*

*Demonstração.* Devemos mostrar que  $\tilde{R}^v y$  é uma realização válida de  $G$ . Iniciamos particionando o conjunto  $E$  em 3 subconjuntos:  $E_1, E_2, E_3$ , onde  $E_1 = \{\{t, u\} \in E | t, u < v\}$ ,  $E_2 = \{\{t, u\} \in E | t, u \geq v\}$  e  $E_3 = \{\{t, u\} \in E | t < v \wedge u \geq v\}$ . Para  $E_1$ , temos pela definição de  $\tilde{R}^v$  que  $\|(\tilde{R}^v y)_t - (\tilde{R}^v y)_u\| = \|Iy_t - Iy_u\| = \|y_t - y_u\| = d_{tu}$ , como queríamos. Para  $E_2$ , utilizamos a definição de  $\tilde{R}^v$  e o fato de  $R^v$  ser uma isometria, assim temos:  $\|(\tilde{R}^v y)_t - (\tilde{R}^v y)_u\| = \|R^v y_t - R^v y_u\| = \|y_t - y_u\| = d_{tu}$ , como queríamos. Para  $E_3$ , devemos mostrar que  $\|(\tilde{R}^v y)_t - (\tilde{R}^v y)_u\| = d_{tu}$ , ou seja  $\|Iy_t - R^v y_u\| = d_{tu}$ . Como  $y \in X$ , pelo Lema 2.4, existe um nó folha factível  $\alpha$ , com  $x(\alpha) = y$ . Como  $\Upsilon(y, v)$  é válida, existe  $\eta \in \mathcal{V}_{\rho(v)-1}$  tal que  $x(\eta) = y[\gamma(v)]$  e  $\mu(\beta) = \boxplus$ , para todo  $\beta \in N^+(\eta)$ . Seja  $p(\alpha) \cap \mathcal{V}_{\rho(v)} = \{\beta\}$ , para algum  $\beta \in N^+(\eta)$ . Novamente por  $\Upsilon(y, v)$ , existe pelo menos um nó folha factível  $\alpha'$ , tal que  $p(\alpha') \cap \mathcal{V}_{\rho(v)} = \{\beta'\}$ , para algum  $\beta' \in N^+(\eta) - \{\beta\}$ . Sejam  $\{w\} = p(\alpha) \cap \mathcal{V}_{\rho(u)}$  e  $\{w'\} = p(\alpha') \cap \mathcal{V}_{\rho(u)}$ . Como  $w'$  é factível,  $\|x(w')_t - x(w')_u\| = d_{tu}$ . Temos que  $\eta$  é um antecessor de ambos  $\alpha$  e  $\alpha'$ , no nível  $\rho(v) - 1$ , e  $t < v$ . Logo,  $p(\alpha') \cap \mathcal{V}_{\rho(t)} = p(\alpha) \cap \mathcal{V}_{\rho(t)}$ , o que implica que  $x(w')_t = x(w)_t = y_t$ . Assim,  $\|y_t - y_u\| = d_{tu} = \|y_t - x(w')_u\|$ . Além disso,

como  $\beta' \in p(w') \cap \mathcal{V}_{\rho(v)}$  e  $x(w')$  é a realização de um vértice  $u > v$  que contém o nó  $x(\beta')$  em seu caminho até o nó raiz. Pelo algoritmo BP, passos 25 e 27,  $\lambda(\beta) = 1 - \lambda(\beta')$ . Como  $\alpha$  é factível, em cada vértice  $u' \in V$ , tal que,  $\rho(v) \leq \rho(u') \leq \rho(u)$ , o nó  $\theta \in p(\alpha) \cap \mathcal{V}_{\rho(u')}$  possui  $f \in \{1, 2\}$  subnós factíveis. Pela Proposição 2.1, o nó  $\theta' \in p(\alpha') \cap \mathcal{V}_{\rho(u')}$  possui  $f$  subnós factíveis. Se  $f = 2$ , pelo Corolário 3.4 e Lema 3.1, podemos escolher  $\alpha'$  de forma que, com probabilidade 1,  $\lambda(\theta') = 1 - \lambda(\theta)$ . Se  $f = 1$ , pelo Algoritmo BP, passos 31 e 33, todos os nós mantêm ou trocam o valor de  $\lambda$  do seus antecessores, implicando em  $\lambda(\theta') = 1 - \lambda(\theta)$ . Portanto, segue do Lema 3.1, com probabilidade 1, que  $x(w')_u = R^v y_u$ . Assim, temos  $\|y_t - R^v y_u\| = d_{ut}$ , como queríamos.  $\square$

## 4 Simetria e o número de soluções

Neste capítulo, nosso objetivo é apresentar e esclarecer em detalhes a relação entre as simetrias no espaço de busca e o número de soluções de uma instância *PDGDM* realizável.

Nas Seções 4.1 e 4.2, mapeamos cada solução  $y \in X$  por uma sequência binária  $\chi \in \{0, 1\}^n$  que descreve todo o caminho da realização, desde o nó raiz até seu respectivo nó folha na árvore  $\mathcal{T}$ . Também definimos o Grupo de Reflexões Parciais e apresentamos resultados sobre a cardinalidade do Grupo de Reflexões Parciais e sua relação com a cardinalidade do número de soluções da instância.

Por fim, na Seção 4.3, apresentamos contra-exemplos para o fato de que todas as instâncias *PDGDM* possuem número de soluções dados por potência de dois.

### 4.1 Relação com sequências binárias e o Grupo de Reflexões Parciais

Considerando todos os nós folhas  $\alpha \in \mathcal{V}$  com  $\mu(\alpha) = \boxplus$ , definamos  $\chi(\alpha) = (\lambda(\beta) | \beta \in p(\alpha))$ . Como as realizações em  $X$  são correspondentes com os nós folhas marcados por  $\boxplus$  em  $\mathcal{T}$ , segue do Algoritmo BP, passo 8, que  $\chi$  define uma relação entre  $X$  e  $\{0, 1\}^n$ . A seguir, demonstramos que esta relação é uma função.

**Lema 4.1.** *Com probabilidade 1, a relação  $\chi$  é uma função.*

*Demonstração.* Devemos mostrar que, com probabilidade 1,  $\chi$  está bem definida. Para isso, mostraremos que a probabilidade de  $\chi$  não ser bem definida é zero. Note que para  $\chi$  não ser bem definida, deve existir uma realização  $x$  que esteja relacionada com duas sequências distintas  $\chi', \chi''$ . Isso corresponde ao discriminante da equação quadrática na prova do Lema 2.1 assumir o valor zero em algum nível maior do 3, o que acontece com probabilidade zero. Portanto, com probabilidade 1,  $\chi$  está bem definida.  $\square$

Seja  $\Xi = \{\chi(y) | y \in X\}$ . Para  $y \in X$ , seja  $y^i$  sua subsequência  $(x_1, \dots, x_i)$ . Para estendermos  $\chi$  sobre todas tais subsequências, colocamos  $\chi^i = (\chi(y)_1, \dots, \chi(y)_i)$ , onde  $\chi(y)$  é válida, se  $y$  é uma realização válida.

Sejam  $N = \{1, \dots, n\}$  e  $g$  a matriz binária  $n \times n$  tal que  $g_{ij} = 1$ , se  $i \leq j$ , e 0 caso contrário, isto é, uma matriz triangular superior com todas as entradas acima da diagonal principal composta por 1. Seja  $g_i$  o seu  $i$ -ésimo vetor linha e  $\Gamma = \{g_i | i \in N\}$ .



Além disso, consideremos o conjunto  $\mathbb{F}_2^n$  composto por  $n$ -uplas de uns e zeros munido da operação de adição elemento a elemento módulo 2, denotada por  $\oplus$ . A seguir, apresentamos alguns resultados técnicos necessários para o desenvolvimento do capítulo. O primeiro garante que  $\mathbb{F}_2^n$  equipado com a operação  $\oplus$  é um grupo aditivo isomorfo a  $C_2^n$ , isto é, o produto cartesiano de  $n$  cópias do grupo cíclico de ordem 2.

**Proposição 4.1.** *O conjunto  $\mathbb{F}_2^n$ , munido da operação  $\oplus$ , tem a estrutura de um grupo aditivo abeliano com identidade  $e = (0, \dots, 0)$ , onde cada elemento é idempotente. Além disso,  $(\mathbb{F}_2^n, \oplus) \cong C_2^n$ .*

*Demonstração.* Devemos mostrar que  $(\mathbb{F}_2^n, \oplus)$  satisfaz as propriedades associativa, comutativa, existência de elemento neutro e existência de elemento inverso. Sejam  $g_i, g_j, g_l \in \mathbb{F}_2^n$ , onde  $g_i = (x_{i_1}, \dots, x_{i_n})$ ,  $g_j = (x_{j_1}, \dots, x_{j_n})$ ,  $g_l = (x_{l_1}, \dots, x_{l_n})$ , com  $x_{i_r}, x_{j_r}, x_{l_r} = 0$  ou 1 para todo  $r = 1, \dots, n$ . Iniciaremos verificando a propriedade associativa:

$$\begin{aligned}
 g_i \oplus (g_j \oplus g_l) &= g_i \oplus ((x_{j_1}, \dots, x_{j_n}) \oplus (x_{l_1}, \dots, x_{l_n})) \\
 &= (x_{i_1}, \dots, x_{i_n}) \oplus (\overline{x_{j_1} + x_{l_1}}, \dots, \overline{x_{j_n} + x_{l_n}}) \\
 &= (\overline{x_{i_1} + (x_{j_1} + x_{l_1})}, \dots, \overline{x_{i_n} + (x_{j_n} + x_{l_n})}) \\
 &= (\overline{(x_{i_1} + x_{j_1}) + x_{l_1}}, \dots, \overline{(x_{i_n} + x_{j_n}) + x_{l_n}}) \\
 &= (\overline{x_{i_1} + x_{j_1}}, \dots, \overline{x_{i_n} + x_{j_n}}) \oplus (x_{l_1}, \dots, x_{l_n}) \\
 &= ((x_{i_1}, \dots, x_{i_n}) \oplus (x_{j_1}, \dots, x_{j_n})) \oplus g_l \\
 &= (g_i \oplus g_j) \oplus g_l
 \end{aligned}$$

Agora, vamos verificar a propriedade comutativa.

$$\begin{aligned}
 g_i \oplus g_j &= (x_{i_1}, \dots, x_{i_n}) \oplus (x_{j_1}, \dots, x_{j_n}) \\
 &= (\overline{x_{i_1} + x_{j_1}}, \dots, \overline{x_{i_n} + x_{j_n}}) \\
 &= (\overline{x_{j_1} + x_{i_1}}, \dots, \overline{x_{j_n} + x_{i_n}}) \\
 &= (x_{j_1}, \dots, x_{j_n}) \oplus (x_{i_1}, \dots, x_{i_n}) \\
 &= g_j \oplus g_i
 \end{aligned}$$

Seguimos verificando a existência do elemento neutro. Como a propriedade comutativa é válida, basta mostrar verificar que para todo  $g_i \in \mathbb{F}_2^n$ ,  $g_i \oplus e = g_i$ . De fato:

$$\begin{aligned}
 g_i \oplus e &= (x_{i_1}, \dots, x_{i_n}) \oplus (0, \dots, 0) \\
 &= (\overline{x_{i_1} + 0}, \dots, \overline{x_{i_n} + 0}) \\
 &= (\overline{x_{i_1}}, \dots, \overline{x_{i_n}}) \\
 &= (x_{i_1}, \dots, x_{i_n}) \\
 &= g_i.
 \end{aligned}$$

Além disso, temos que

$$\begin{aligned} g_i \oplus g_i &= (x_{i_1}, \dots, x_{i_n}) \oplus (x_{i_1}, \dots, x_{i_n}) \\ &= (\overline{x_{i_1} + x_{i_1}}, \dots, \overline{x_{i_n} + x_{i_n}}), \end{aligned}$$

para todo  $r = 1, \dots, n$ . Como  $x_{i_r} = 0 \Rightarrow \overline{x_{i_r} + x_{i_r}} = \overline{0 + 0} = \overline{0} = 0$  e  $x_{i_r} = 1 \Rightarrow \overline{x_{i_r} + x_{i_r}} = \overline{1 + 1} = \overline{2} = 0$ , segue que

$$g_i \oplus g_i = (0, \dots, 0) = e.$$

Logo,  $g_i^{-1} = g_i$  e a propriedade de existência do elemento inverso é satisfeita. Além disso, como  $g_i^2 = e$ , temos que os elementos de  $(\mathbb{F}_2^n, \oplus)$  são idempotentes. Como todo grupo cíclico de ordem 2 é isomorfo a  $\mathbb{Z}_2$ , temos que  $C_2^n \cong \mathbb{Z}_2^n$ . Assim, definamos:

$$\begin{aligned} \psi : (\mathbb{F}_2^n, \oplus) &\rightarrow \mathbb{Z}_2^n \\ g_i = (x_{i_1}, \dots, x_{i_n}) &\rightarrow (x_{i_1}, \dots, x_{i_n}) \end{aligned}$$

Vamos agora mostrar que  $\psi$  é um homomorfismo, ou seja,  $\psi(g_i \oplus g_j) = \psi(g_i) \oplus \psi(g_j)$ . De fato:

$$\begin{aligned} \psi(g_i \oplus g_j) &= \psi((x_{i_1}, \dots, x_{i_n}) \oplus (x_{j_1}, \dots, x_{j_n})) \\ &= \psi(\overline{x_{i_1} + x_{j_1}}, \dots, \overline{x_{i_n} + x_{j_n}}) \\ &= (\overline{x_{i_1} + x_{j_1}}, \dots, \overline{x_{i_n} + x_{j_n}}) \\ &= (x_{i_1}, \dots, x_{i_n}) \oplus (x_{j_1}, \dots, x_{j_n}) \\ &= \psi(x_{i_1}, \dots, x_{i_n}) \oplus \psi(x_{j_1}, \dots, x_{j_n}) \\ &= \psi(g_i) \oplus \psi(g_j). \end{aligned}$$

Seguimos demonstrando que  $\psi$  é injetora. De fato:

$$\begin{aligned} \psi(g_i) = \psi(g_j) &\Leftrightarrow \psi(x_{i_1}, \dots, x_{i_n}) = \psi(x_{j_1}, \dots, x_{j_n}) \\ &\Leftrightarrow (x_{i_1}, \dots, x_{i_n}) = (x_{j_1}, \dots, x_{j_n}) \\ &\Leftrightarrow g_i = g_j. \end{aligned}$$

Além disso,  $\psi$  é também sobrejetora, pois dado  $(x_1, \dots, x_n) \in \mathbb{Z}_2^n$ , tome  $g_r = (x_{r_1}, \dots, x_{r_n}) \in \mathbb{F}_2^n$ , onde  $x_{r_j} = x_j$  para todo  $j = 1, \dots, n$ , e

$$\psi(g_r) = \psi(x_{r_1}, \dots, x_{r_n}) = (x_{r_1}, \dots, x_{r_n}) = (x_1, \dots, x_n).$$

Obtemos então que  $\psi$  é um isomorfismo entre  $(\mathbb{F}_2^n, \oplus)$  e  $\mathbb{Z}_2^n$ , o que conclui a demonstração.  $\square$

Nos próximos resultados, apresentamos informações sobre a ação do grupo  $(\mathbb{F}_2^n, \oplus)$  e sobre um dos seus conjuntos de geradores.

**Proposição 4.2.** *O grupo  $(\mathbb{F}_2^n, \oplus)$  age sobre si mesmo pela mesma operação  $\oplus$ .*

*Demonstração.* Defina

$$\begin{aligned} f : (\mathbb{F}_2^n, \oplus) &\rightarrow \mathcal{P}(\mathbb{F}_2^n) \\ g_i &\rightarrow f_{g_i}, \end{aligned}$$

onde  $f_{g_i} : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  é definida como  $f_{g_i}(g_j) = g_i \oplus g_j$ .

Iniciamos verificando que  $f_{g_i} \in \mathcal{P}(\mathbb{F}_2^n)$  é injetora. De fato, dados  $g_j, g_l \in \mathbb{F}_2^n$  tais que  $f_{g_i}(g_j) = f_{g_i}(g_l)$ , temos

$$\begin{aligned} f_{g_i}(g_j) = f_{g_i}(g_l) &\Rightarrow g_i \oplus g_j = g_i \oplus g_l \\ &\Rightarrow g_i^{-1} \oplus g_i \oplus g_j = g_i^{-1} \oplus g_i \oplus g_l \\ &\Rightarrow g_j = g_l. \end{aligned}$$

Além disso, dado  $g_j \in \mathbb{F}_2^n$ , considere  $g_i \oplus g_j \in \mathbb{F}_2^n$ . Pela idempotência dos elementos de  $(\mathbb{F}_2^n, \oplus)$ , temos

$$f_{g_i}(g_i \oplus g_j) = g_i \oplus (g_i \oplus g_j) = g_i^2 \oplus g_j = g_j.$$

Vamos mostrar agora que  $f : (\mathbb{F}_2^n, \oplus) \rightarrow \mathcal{P}(\mathbb{F}_2^n)$  é um homomorfismo. De fato,

$$\begin{aligned} f(g_i \oplus g_j) = f(g_i) \oplus f(g_j) &\Leftrightarrow f_{g_i \oplus g_j}(g_l) = f_{g_i} \oplus f_{g_j}(g_l), \quad \forall g_l \in \mathbb{F}_2^n \\ &\Leftrightarrow (g_i \oplus g_j) \oplus g_l = g_i \oplus (g_j \oplus g_l), \end{aligned}$$

o que é válido pela propriedade associativa do grupo  $(\mathbb{F}_2^n, \oplus)$ . Portanto,  $f$  é uma ação de  $(\mathbb{F}_2^n, \oplus)$  no conjunto  $\mathbb{F}_2^n$ , como queríamos demonstrar.  $\square$

**Proposição 4.3.** *O conjunto  $\Gamma$  é um conjunto gerador do grupo  $(\mathbb{F}_2^n, \oplus)$ . Além disso, o conjunto  $\Gamma$  é linearmente independente no espaço vetorial  $\nu$  gerado por  $(\mathbb{F}_2^n, \oplus)$ , com multiplicação por escalar definida sobre o corpo  $\mathbb{F}_2$ .*

*Demonstração.* Seja  $g_S \in (\mathbb{F}_2^n, \oplus)$ . Então,  $g_S = (x_{S_1}, \dots, x_{S_n})$ , onde  $x_{S_j} = 1$  ou  $0$ ,  $\forall j = 1, \dots, n$ . Considere  $g_{w_1} \oplus \dots \oplus g_{w_n}$ , com  $g_{w_l} \in \Gamma$ ,  $\forall l = 1, \dots, n$ . Temos que:

$$\begin{aligned} \text{Se } l = n, \text{ então } g_{w_n} &= \begin{cases} g_n & \text{se } x_{S_n} = 1 \\ e & \text{se } x_{S_n} = 0 \end{cases} \\ \text{Se } l < n, \text{ então } g_{w_l} &= \begin{cases} g_l & \text{se } x_{S_l} = 1 \wedge x_{S_{l+1}} = 0 \\ e & \text{se } x_{S_l} = 1 \wedge x_{S_{l+1}} = 1 \\ g_l & \text{se } x_{S_l} = 0 \wedge x_{S_{l+1}} = 1 \end{cases} \end{aligned}$$

Desta forma, obtemos  $g_S = g_{w_1} \oplus \dots \oplus g_{w_l}$ , ou seja,  $\Gamma$  é um conjunto gerador do grupo  $(\mathbb{F}_2^n, \oplus)$ . Se  $a_1, \dots, a_n \in \mathbb{F}_2$ , temos:

$$\begin{aligned} a_1 g_1 \oplus \dots \oplus a_n g_n = 0 &\Rightarrow a_1(1, 0, \dots, 0) \oplus \dots \oplus a_n(1, 1, \dots, 1) = 0 \\ &\Rightarrow (a_1, 0, \dots, 0) \oplus \dots \oplus (a_n, \dots, a_n) = 0 \\ &\Rightarrow (\overline{a_1 + \dots + a_n}, \overline{a_2 + \dots + a_n}, \dots, \overline{a_n}) = 0 \\ &\Rightarrow a_n = a_{n-1} = \dots = a_1 = 0. \end{aligned}$$

Portanto, o conjunto  $\Gamma$  é linearmente independente no espaço vetorial  $\nu$ , o que conclui a demonstração.  $\square$

Vamos estabelecer uma aplicação entre o conjunto das partes de  $N$  e o grupo  $(\mathbb{F}_2^n, \oplus)$ . Para cada  $S \subseteq N$ , seja

$$g_S = \bigoplus_{i \in S} g_i,$$

e definimos a aplicação  $\phi : \mathcal{P}(N) \rightarrow (\mathbb{F}_2^n, \oplus)$  dada por  $\phi(S) = g_S$ .

**Lema 4.2.** *A aplicação  $\phi$  é injetora.*

*Demonstração.* Mostraremos que, dados  $S, T \subseteq N$ , se  $g_S = g_T$ , então  $S = T$ . De fato:

$$\begin{aligned} g_S &= g_T \\ \Rightarrow \bigoplus_{i \in S} g_i &= \bigoplus_{i \in T} g_i \\ \Rightarrow \bigoplus_{i \in S} g_i \oplus \left( \bigoplus_{i \in T} g_i \right)^{-1} &= e. \end{aligned}$$

Pela propriedade comutativa:

$$\bigoplus_{i \in T} g_i \oplus \bigoplus_{i \in T} g_i^{-1} = \bigoplus_{i \in T} g_i \oplus g_i^{-1} = \bigoplus_{i \in T} e = e,$$

implicando em

$$\bigoplus_{i \in T} g_i^{-1} = \left( \bigoplus_{i \in T} g_i \right)^{-1}.$$

Pela propriedade da idempotência, temos que  $g_i = g_i^{-1}$ . Assim, segue que

$$\bigoplus_{i \in S} g_i \oplus \bigoplus_{i \in T} g_i = e.$$

Para  $i \in S \cap T$ , temos que  $g_i \oplus g_i = g_i^2$ . Assim,

$$\bigoplus_{i \in S \Delta T} g_i \oplus \bigoplus_{i \in S \cap T} g_i^2 = e.$$

Pela idempotência dos elementos, obtemos:

$$\bigoplus_{i \in S \Delta T} g_i = e.$$

Como os elementos são linearmente independentes, temos que

$$S \Delta T = e \Rightarrow S = T,$$

que conclui a demonstração.  $\square$

Seja  $I$  o conjunto de níveis de  $\mathcal{T}$  para os quais todos os níveis a seguir, com dois subnós factíveis, possuem caminhos até os nós folhas factíveis para ambos os subnós. Seja  $L = \{g_i \in \Gamma \mid i \in I\}$  e  $\Lambda = \langle L \rangle$  o subgrupo de  $(\mathbb{F}_2^n, \oplus)$  gerado por  $L$ . Definimos este subgrupo como o **Grupo das Representações Parciais**.

## 4.2 Cardinalidade do Conjunto de Soluções

Iniciamos esta seção apresentando um resultado que, essencialmente, mostra que a cardinalidade do grupo de reflexões parciais é uma potência de 2.

**Lema 4.3.** *Para todo  $H \subset \Gamma$ ,  $|\langle H \rangle| = 2^{|H|}$ .*

*Demonstração.* Vamos mostrar que  $\phi$  é uma bijeção entre  $\mathcal{P}(H)$  e  $\langle H \rangle$ . Pelo Lema 4.2, a restrição da função  $\phi$  a  $\mathcal{P}(H)$  é injetiva. Além disso, dado um elemento  $g \in \langle H \rangle$ , este pode ser escrito como  $\bigoplus_{i \in S} g_i$ , para algum  $S \subseteq H$ , pois  $H$  é o conjunto gerador para o espaço vetorial  $H$  sobre  $\mathbb{F}_2^n$ , o qual é como conjunto igual ao grupo  $\langle H \rangle$ . Assim,  $\phi$  é sobrejetiva também. Portanto,  $\phi$  é uma bijeção entre  $\mathcal{P}(H)$  e  $\langle H \rangle$ , como queríamos demonstrar.  $\square$

**Teorema 4.1.** *Se  $\Xi \neq \emptyset$ , para todo  $\xi \in \Xi$ , temos, com probabilidade 1,  $\xi \oplus \Lambda = \Xi$ .*

*Demonstração.* Primeiramente, demonstraremos que  $\xi \oplus \Lambda \subseteq \Xi$ , com probabilidade 1. Como  $\langle L \rangle = \Lambda$ , é suficiente mostrar que  $\xi \oplus g_i \in \Xi$  para um arbitrário  $g_i \in L$ , ou seja, devemos mostrar que existe uma realização válida  $w \in X$  satisfazendo  $\chi(w) = \xi \oplus g_i$ . Sejam  $y \in \chi^{-1}(\xi)$  e  $v = \rho^{-1}(i)$  satisfazendo  $\Upsilon(y, v)$ . Defina  $w = \tilde{R}^v y$ . Pelo Teorema 3.1,  $w \in X$ . Seja  $\alpha'$  o nó folha de  $\mathcal{T}$  tal que  $x(\alpha') = y$ . Pelo Lema 2.4, existe um nó folha  $\beta'$  tal que  $x(\beta') = w$ . Agora, precisamos mostrar que para todo  $l \geq i$ , o nó  $\beta \in p(\beta') \cap \mathcal{V}_l$  satisfaz  $\lambda(\beta) = 1 - \lambda(\alpha)$ , onde  $\alpha$  é o nó pertencente a  $p(\alpha') \cap \mathcal{V}_l$ . Para isso, utilizaremos indução sobre  $l$ . Para  $l = i$ , pelo Lema 2.3, temos que a realização do nó  $\beta$  é uma reflexão da realização do nó  $\alpha$ . Assim, pelo Lema 3.1, temos  $\lambda(\beta) = 1 - \lambda(\alpha)$ . Para  $l > i$ , pela hipótese de indução nos níveis  $i \leq r < l$ ,  $\lambda(\beta) = 1 - \lambda(\alpha)$ , onde  $\beta \in p(\beta') \cap \mathcal{V}_r$ , e  $\alpha \in p(\alpha') \cap \mathcal{V}_r$ . Pelo Lema 3.1,  $x(\beta)_{\rho^{-1}(r)} = R^v x(\alpha)_{\rho^{-1}(r)}$ . E, além disso,  $w = \tilde{R}^v y$ . Assim, para  $\beta \in p(\beta') \cap \mathcal{V}_l$  e  $\alpha \in p(\alpha') \cap \mathcal{V}_l$ , temos  $x(\beta)_{\rho^{-1}(l)} = R^v x(\alpha)_{\rho^{-1}(l)}$ . Novamente pelo Lema 3.1, o evento  $\lambda(\beta) = 1 - \lambda(\alpha)$  ocorre com probabilidade 1.

Agora, mostraremos que  $\Xi \subseteq \xi \oplus \Lambda$ , com probabilidade 1, ou seja, para qualquer  $\eta \in \Xi$ , existe  $g \in \Lambda$  satisfazendo  $\xi \oplus g = \eta$ . Procedemos por indução sobre  $n$ , iniciando quando  $n = 4$ . Se  $4 \notin I$  então  $|\Xi| = 1$ ,  $L = \emptyset$  e o resultado é válido. Se  $4 \in I$ , então  $|\Xi| = 2$ ,  $L = \{g_4\}$  e o resultado é válido. Seja  $n > 4$ , para todo  $j \in \{4, \dots, n-1\}$  e defina  $\Xi^j = \{\xi^j | \xi \in \Xi\}$  e  $L^j = \{g_l \in \Gamma | l \in I \wedge l \leq j\}$ . Pela hipótese de indução, para todo  $\xi' \in \Xi^j$ , temos  $\xi' \oplus \langle L^j \rangle = \Xi^j$ . Note que  $n \notin I$  ou  $n \in I$ . Pela Proposição 2.1, se  $n \notin I$ , então, com probabilidade 1,  $\mathcal{V}_{n-1}$  pode somente ter 0 ou 1 subnó factível. Seja  $B_1^n$  o conjunto de todos tais subnós factíveis. Se  $n \in I$ , então  $\mathcal{V}_{n-1}$  admite somente 0 ou 2 subnós factíveis. Seja  $B_2^n$  o conjunto de todos tais subnós factíveis. No primeiro caso, sejam  $\Xi^n = \{\xi(x(\beta)) | \beta \in B_1^n\}$ ,  $L^n = L^{n-1}$ . Assim, pela hipótese de indução, temos que para os níveis anteriores de  $n$ , o resultado é válido e, para o nível  $n$ , temos somente um nó factível para cada ramo da árvore no nível  $n-1$ , que possui subnó. Portanto,  $L^n = L^{n-1}$  satisfaz para todo  $\xi' \in \Xi^n$ ,  $\xi' \oplus \langle L^n \rangle = \Xi^n$  e este caso segue. No segundo caso, seja  $\Xi^n = \{\xi(x(\beta)) | \beta \in B_2^n\}$  e  $L^n = L^{n-1} \cup \{g_n\}$ . Assim, como

$g_n = (0, \dots, 1)$ , dado  $\eta \in \Xi$  e  $n \in I$ , pela hipótese de indução e pela idempotência de  $g_n$ , temos que existe  $g_S \in L^{n-1}$  tal que  $\eta = \xi \oplus g_S \oplus g_n^t$ , onde  $t = 1$  ou  $t = 2$ . Portanto, este caso também é válido e assim concluímos a demonstração do resultado.  $\square$

**Corolário 4.1.** *Se uma instância PDGDM é realizável, então, com probabilidade 1,  $|X|$  é uma potência de 2.*

*Demonstração.* Considerando  $\chi : X \rightarrow \{0, 1\}^n$ , definida por  $\chi(\alpha) = (\lambda(\beta) | \beta \in p(\alpha))$ , pelo Lema 4.1,  $\chi$  é uma função com probabilidade 1. Sejam  $x, x' \in X$  distintos. Pelo Algoritmo BP, passos 25, 27, 31 e 33,  $\chi(x), \chi(x')$  são distintos. Assim, a função  $\chi : X \rightarrow \Xi$  é injetiva. Como, por definição,  $\Xi = \{\chi(y) | y \in X\}$ , a função  $\chi : X \rightarrow \Xi$  é sobrejetiva. Assim,  $|X| = |\Xi|$ , pelo Teorema 4.1, com probabilidade 1, para todo  $\chi \in \Xi$ ,  $|\Xi| = |\chi \oplus \Lambda|$ . Além disso,  $|\chi \oplus \Lambda| = |\Lambda|$ . De fato, considere  $f : \Lambda \rightarrow \chi \oplus \Lambda$ , definida por  $f(g_S) = \chi \oplus g_S$ . Inicialmente, mostraremos que  $f$  é injetiva, ou seja, se  $\chi \oplus g_S = \chi \oplus g_T$ , então  $g_S = g_T$ :

$$\begin{aligned}
& \chi \oplus g_S &= \chi \oplus g_T \\
\Rightarrow & \chi \oplus \bigoplus_{i \in S} g_i &= \chi \oplus \bigoplus_{i \in T} g_i \\
\Rightarrow & \chi \oplus \bigoplus_{i \in S} \bigoplus_{i \in T} g_i^{-1} &= \chi \\
\Rightarrow & \bigoplus_{i \in S} g_i \oplus \bigoplus_{i \in T} g_i^{-1} &= e \\
\Rightarrow & \bigoplus_{i \in S} g_i &= \bigoplus_{i \in T} g_i \\
\Rightarrow & g_S &= g_T.
\end{aligned}$$

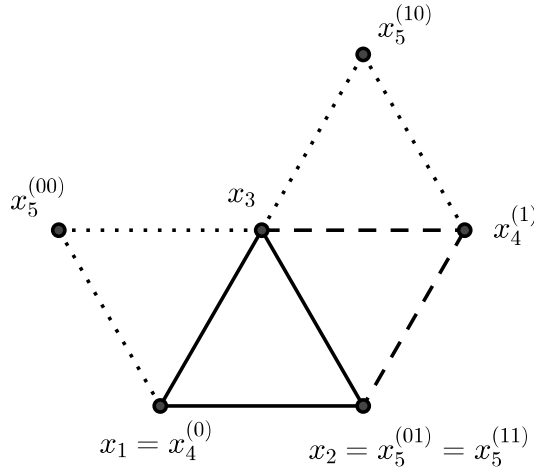
Dado  $\chi \oplus g_S \in \chi \oplus \Lambda$ , considere  $g_S \in \Lambda$ , implicando em  $f(g_S) = \chi \oplus g_S$ . Logo,  $f$  é também sobrejetora. Como consequência, existe uma bijeção entre  $\Lambda$  e  $\chi \oplus \Lambda$  e, portanto,  $|\Lambda| = |\chi \oplus \Lambda|$ . Pelo Lema 4.3, com probabilidade 1,  $|X|$  é, então, uma potência de 2, como queríamos demonstrar.  $\square$

### 4.3 Contra-exemplos

Nesta seção, apresentamos uma classe de instâncias PDGDM que não possui número de soluções sendo uma potência de 2. Apresentamos também um contra-exemplo que ilustra que a generalização dos resultados para o PDGD<sub>3</sub> não é trivial.

Todos os contra-exemplos são construídos artificialmente, com a propriedade que duas realizações distintas  $x, x'$  possuem, no mínimo, um nível  $i$  onde  $x_i = x'_i$ , com probabilidade 0.

**Contra-exemplo 4.2.** *Para  $K = 3$ , seja  $n = 6$ ,  $V = \{1, \dots, 6\}$ ,  $E = \{\{i, j\} | 0 < i - j \leq 3\} \cup \{\{1, 6\}\}$  e  $d_{ij} = 1$ , para todo  $\{i, j\} \in E$ . Os primeiros  $n - 2 = 4$  vértices podem ser realizados como vértices de um simplex regular de dimensão 3. Note agora que o vértice  $x_5$*



(a) Posição dos pontos no plano.

Figura 6 – Ilustração do contra-exemplo 4.2 para  $K = 2$ . Note que os nós  $x_5^{(00)}$ ,  $x_5^{(01)}$ ,  $x_5^{(11)}$  são factíveis. Entretanto, o nó  $x_5^{(10)}$  não satisfaz  $d_{1,5}$ .

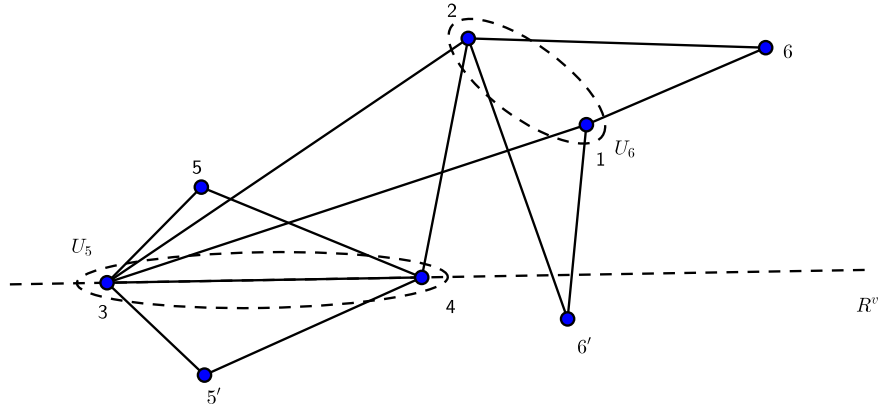


Figura 7 – Um contra-exemplo para o Lema 3.1 quando aplicado em  $PDGD_3 \setminus PDGDM$ , também para  $K = 2$ .

pode ser realizado como  $x_5 = x_1$ , pois possui as 3 arestas com pesos e pares coincidindo com as de  $x_1$ , ou  $x_5$  está na posição simétrica a de  $x_1$  com relação ao plano através dos pontos  $\{x_2, x_3, x_4\}$ . No primeiro caso, temos dois nós factíveis possíveis para  $x_6$ , sendo eles  $x_2$  e seu simétrico com relação ao plano através dos pontos  $\{x_3, x_4, x_5\}$ . No segundo caso, somente  $x_6 = x_2$  é um nó factível, pois a posição do nó simétrico a  $x_2$  não satisfaz a distância  $d_{1n} = 1$ . Para o caso em que a dimensão é  $K = 2$ , a ilustração é apresentada na Figura 6.

**Contra-exemplo 4.3** ("Necessidade" de antecessores imediatos). A Figura 7 apresenta um contra-exemplo onde a implicação  $(2) \rightarrow (1)$  do Lema 3.1 falha para instâncias em  $PDGD_3 \setminus PDGDM$ , implicando que a generalização dos resultados apresentados para

o PDGDM é muito complicada. Seja  $V = \{1, \dots, 6\}$  os vértices do grafo realizado na Figura 7. Note que os pontos  $5', 6'$  mostram nós factíveis alternativos para os vértices 5, 6. Sejam  $U_5 = \{3, 4\}$  e  $U_6 = \{1, 2\}$  os vértices adjacentes de 5 e 6, respectivamente. A linha através dos pontos 3, 4 não gera uma reflexão factível para o nó  $6'$  do vértice 6. Isto acontece por  $U_6$  não conter os antecessores imediatos do vértice 6.



## 5 O Algoritmo iBP

Neste Capítulo, apresentamos generalizações de diversos resultados apresentados nos capítulos anteriores, com o intuito de tornar o problema mais próximo de situações da realidade. Na Seção 5.1, apresentamos uma nova ordem que torna o Algoritmo BP aplicável em problemas envolvendo estruturas de proteínas. Na Seção 5.2, apresentamos as generalizações dos resultados dos Capítulos 2 e 3, com as devidas alterações. Na Seção 5.3, é feita uma estimativa da cardinalidade do conjunto solução do problema generalizado.

### 5.1 Nova Ordem nos Vértices

Nesta seção, estamos interessados em tornar o Algoritmo BP mais realista e utilizável em problemas de estrutura de proteínas. Consideremos um grafo  $G = (V, E, d)$  de um PDGDM associado a uma proteína.

Dado um vértice  $v \in V$ , denotamos por  $v - h$  o vértice de nível  $\rho(v) - h$  para algum  $h < \rho(v)$ . As distâncias entre átomos conectados por ligações covalentes e seus ângulos são conhecidos com precisão aceitável. Assim, consideramos as distâncias  $d_{v-1,v}, d_{v-2,v}$  exatas para qualquer vértice  $v$  tal que  $\rho(v) > 3$ . As distâncias  $d_{v-3,v}$ , bem como outras distâncias relativas a átomos próximos detectados por experimentos de RMN, podem não possuir valores exatos.

Motivados pelas observações acima, definimos então uma ordem em  $V$  tal que,  $\forall v \in V, \rho(v) > 3$ , temos:

- $d_{v-2,v}, d_{v-1,v}$  são valores exatos em  $\mathbb{R}_+$ ,
- $d_{v-3,v}$  é um valor exato ou um conjunto finito  $\{d_{uv}^1, \dots, d_{uv}^q\}$ , onde  $q > 1$ , valores em  $\mathbb{R}_+$ ,
- $d_{uv}$  é um valor exato, ou um intervalo  $[d_{uv}^L, d_{uv}^U]$ , para todo  $\rho(u) < \rho(v) - 3$ .

Note que esta ordem utiliza as distâncias intervalares somente para realizar podas na árvore de busca, já que a discretização do espaço de busca ocorre de forma semelhante ao modelo anterior, pois a distância  $d_{v-3,v}$  um valor exato, ou um conjunto finito de valores exatos.

## 5.2 Algoritmo *iBP*

Assuma que  $v \in V$  é tal que  $d_{v-3,v}$  é um conjunto de  $q$  valores reais positivos e todas as outras distâncias são precisas. Então, o Lema 2.1 tem a seguinte extensão:

**Lema 5.1.** *Se  $|N(v) \cap \gamma(v)| = 3$ , então existem no máximo  $2q$  extensões distintas de  $x$  que são válidas para  $G^v$ . Se existe uma extensão válida, então, com probabilidade 1, existem exatamente  $2q$  extensões válidas distintas.*

*Demonstração.* Como  $|N(v) \cap \gamma(v)| = 3$ , então  $U_v = N(v) \cap \gamma(v) = \{v-1, v-2, v-3\}$ . Tomando  $v-3 \in U_v$ , temos que a equação (2.2) é dada por

$$\forall u \in U_v - \{v-3\}, (\|z - x_u\| = d_{uv}) \text{ e } (\|z - x_{v-3}\| \in d_{v-3,v})$$

e a terceira linha da Equação (2.3) é dada por;

$$\|z\|^2 - 2x_{v-3} \cdot z + \|x_{v-3}\|^2 \in d_{v-3,v}^2,$$

onde  $d_{v-3,v}^2$  denota o conjunto  $\{(d_{v-3,v}^j)^2 | j \leq q\}$  das  $q$  distâncias  $d_{v-3,v}$ . Temos então,  $q$  diferentes equações quadráticas

$$\|z\|^2 - 2x_w \cdot z + \|x_w\|^2 = (d_{wv}^j)^2, \quad (5.1)$$

onde  $j \leq q$ . Para cada uma dessas equações, segue pelo Lema 2.1 que existem dois diferentes valores para  $z$  com probabilidade 1, como queríamos demonstrar.  $\square$

O próximo resultado é idêntico ao Lema 2.2, mas a demonstração é diferente.

**Lema 5.2.** *Se  $|N(v) \cap \gamma(v)| > 3$  então, com probabilidade 1, existe no máximo uma extensão válida de  $x$ .*

*Demonstração.* Como  $U_v \subseteq N(v) \cap \gamma(v)$ , somente considerando vértices em  $U_v$  estamos na situação do Lema 5.1 e temos  $2q$  possibilidades de extensão de  $x$ . Agora, considere um antecessor adjacente  $u$  de  $v$  que não pertence a  $U_v$ . Com probabilidade 1, as distâncias  $\|x_u - z^{1j}\|, \|x_u - z^{2j}\|$ , onde  $z^{1j}, z^{2j}$  são os dois nós do vértice  $v$  com relação a distância  $d_{v-3,v}^j$ , são todas distintas, para  $j \leq q$ . Portanto, no máximo, apenas uma pode ser igual a  $d_{uv}$ .  $\square$

O próximo resultado é uma generalização do Lema 2.3.

**Lema 5.3.** *Seja  $\bar{x}$  uma realização válida de  $G[U_v]$  e sejam  $\{z^{1j}, z^{2j} | j \leq q\} \subseteq \mathbb{R}^3$  as  $2q$  posições do vértice  $v$  dadas pelo Lema 5.1, onde  $z^{1j}, z^{2j}$  são obtidas da equação (5.1), indexadas por  $j$ . Então,  $z^{2j}$  é uma reflexão de  $z^{1j}$  com respeito ao plano dado pelos 3 pontos de  $\bar{x}$ .*

*Demonstração.* Como qualquer esfera em  $\mathbb{R}^3$  é simétrica com respeito a qualquer plano passando pelo seu centro, a interseção de 3 esferas é simétrica ao plano através dos seus 3 centros. Assim, para cada valor  $d_{uv}^j$ , temos que  $z^{2j}$  é simétrico a  $z^{1j}$  para cada  $j \leq q$ .  $\square$

Devido às mudanças no Lema 5.3, o algoritmo BP é influenciado em vários aspectos. A mudança mais importante é que se  $d_{v-3,v}$  é um conjunto e  $v$  possui 3 antecessores adjacentes, o nó  $\alpha$  no nível  $v - 1$  da árvore do **iBP** tem exatamente  $2q$  subnós  $z^{ij}$ , onde  $i \in \{1, 2\}$ ,  $j \leq q$ , no nível  $v$ . Desta forma, para todo  $i \in \{1, 2\}$  e  $j \leq q$ ,  $\lambda(\alpha^{ij})$  é definido da seguinte forma:

$$\lambda(\alpha^{ij}) = \begin{cases} -j & \text{se } a_v^\top z^{ij} \leq a_{v0} \\ j & \text{se } a_v^\top z^{ij} > a_{v0} \end{cases} \quad (5.2)$$

Assim, temos as seguintes mudanças no Algoritmo BP: o conjunto  $Z$ , no passo 17, é  $\{z^{ij} | i \in \{1, 2\} \wedge j \leq q\}$ ; o teste no passo 23 é  $|Z| = 2q$ ; e o código do correspondente se muda da seguinte forma:

```

para  $j \leq q$  fazer
  se  $a_v^\top z^{1j} \leq a_{v0}$  então
    Sejam  $\alpha^{1j} = (z^{1j}, -j, \boxplus)$ ,  $\alpha^{2j} = (z^{2j}, j, \boxplus)$ 
  senão
    Sejam  $\alpha^{1j} = (z^{1j}, j, \boxplus)$ ,  $\alpha^{2j} = (z^{2j}, -j, \boxplus)$ 
  fim se
fim para

```

Observamos que a árvore de busca do iBP não é mais uma árvore de busca binária, pois  $d_{v-3,v}$  pode assumir um conjunto finito de valores reais positivos. Sempre que isto ocorre, o nó no nível  $v - 1$  possui  $2q$  subnós. O número total de nós no iBP depende do número de vezes que  $d_{v-3,v}$  deixa de ser um único valor.

Prosseguimos com as alterações na Proposição 2.1, cuja mudança é consequências de termos, com probabilidade 1, pelos Lemas 5.1 e 5.2, uma ou  $2q$  possíveis extensões válidas.

**Proposição 5.1.** *Com probabilidade 1, não existe nenhum nível  $i \leq n$  contendo duas realizações distintas válidas  $\beta, \theta \in \mathcal{V}_i$ , tal que  $|\{\alpha \in N^+(\beta) | \mu(\alpha) = \boxplus\}| = 1$  e  $|\{\alpha \in N^+(\theta) | \mu(\alpha) = \boxplus\}| = 2q$ .*

*Demonstração.* Considere  $T_v = N(v) \cap \gamma(v)$ . Se  $|T_v| = 3$ , pelo Lema 5.1, com probabilidade 1,  $\beta$  tem exatamente  $2q$  subnós realizáveis. Como por hipótese este possui somente 1, então o evento  $|T_v| = 3$  ocorre com probabilidade 0. Como  $|T_v| \geq 3$ , o evento  $|T_v| > 3$  ocorre com probabilidade 1. Assim, pelo Lema 5.2, com probabilidade 1, existe no máximo uma extensão para a realização em  $v$ .  $\square$

### 5.2.1 Geometria na Árvore do iBP

Nesta subseção, vamos apresentar a generalização dos resultados do Capítulo 3. Iniciamos enunciando o Corolário 3.1 para o iBP.

**Corolário 5.1.** *Seja  $\alpha \in \mathcal{V}_{i-1}$ , para algum  $i > 1$ ,  $v = \rho^{-1}(i)$  e  $N^+(\alpha) = \{\eta^{ij} | i \in \{1, 2\} \wedge j \leq q\}$ , com  $\mu(\eta^{ij}) = \boxplus$ , para todo  $i \in \{1, 2\}$ ,  $j \leq q$ . Então,  $x(\eta^{1j})_v = R^v x(\eta^{2j})_v$ .*

*Demonstração.* Pelo Lema 5.3, temos que  $\eta^{1j}$  é reflexão de  $\eta^{2j}$  através do plano dado pelos 3 pontos de  $\bar{x}$ , onde  $\bar{x}$  é qualquer realização válida de  $G[U_v]$ . Ou seja,  $x(\eta^{1j})_v = R^v x(\eta^{2j})_v$ .  $\square$

Apresentamos a seguir um resultado técnico equivalente ao Lema 3.1 para o iBP.

**Lema 5.4.** *Seja  $\alpha \in \mathcal{V}_{i-1}$ , para algum  $i > 1$ , tal que  $N^+(\alpha) = \{\eta', \beta'\}$ ,  $u = \rho^{-1}(i)$  e  $v = \rho^{-1}(l)$  tal que  $l \geq i$  e considere dois nós factíveis  $\eta, \beta \in \mathcal{V}_l$ , tais que  $\{\eta'\} = p(\eta) \cap \mathcal{V}_i$  e  $\{\beta'\} = p(\beta) \cap \mathcal{V}_i$ . Além disso, para todo  $i \leq j \leq l$ , seja  $w = \rho^{-1}(j)$ ,  $p(\eta) \cap \mathcal{V}_i = \{\eta''\}$  e  $p(\beta) \cap \mathcal{V}_i = \{\beta''\}$ . Então, com probabilidade 1, as seguintes afirmações são equivalentes:*

1. Para todo  $i \leq j \leq l$ ,  $x(\eta'')_w = R^u x(\beta'')_w$ ;
2. Para todo  $i \leq j \leq l$ , se  $d_{uw}$  é um único valor, então  $\lambda(\eta'') = 1 - \lambda(\beta'')$ ; e se  $d_{uw}$  é um conjunto, então  $\lambda(\eta'') = -\lambda(\beta'')$ .

*Demonstração.* Sejam  $a_v^{0\top} x = a_{v0}^0$ ,  $a_v^{1\top} x = a_{v0}^1$  as equações dos planos  $H_\eta, H_\beta$ , respectivamente, definidos por  $x(\eta)[U_v]$  e  $x(\beta)[U_v]$ , com vetores normais orientados como descrito na Observação 1.2. Vamos demonstrar por indução sobre  $l$  que a seguinte condição é equivalente a (1) e (2):

3. Para todo  $i \leq j \leq l$ ,  $x(\beta'')_w = R^u x(\eta'')_w$  e  $a_u \cdot a_w^0 = a_u \cdot a_w^1$ , onde  $a_w^0$  e  $a_w^1$  são os vetores normais dos planos  $H_{\eta''}$  e  $H_{\beta''}$  orientados usualmente.

Para  $l = i$ , temos que (1) e (3) valem simultaneamente. De fato, se  $d_{uw}$  é um único valor, o resultado está demonstrado no Lema 3.1, e se  $d_{uw}$  é um conjunto de valores, como  $\eta = \eta'$  e  $\beta = \beta'$ , pelo Lema 5.3,  $x(\beta)_v = R^u x(\eta)_v$ . Pela equação (5.2) segue que  $\lambda(\eta) = -\lambda(\beta)$ . Além disso temos  $H_\eta = R^u H_\beta$ , implicando em  $|a_u \cdot a_v^0| = |a_u \cdot a_v^1|$ . Como a orientação de  $a_v^0$ ,  $a_v^1$  é tal que  $a_u \cdot a_v^0, a_u \cdot a_v^1 \geq 0$ , o resultado é válido para  $l = i$ . Assumindo por hipótese de indução que as equivalências são válidas para o nível  $l - 1$ , mostraremos que o resultado é válido para o nível  $l$ . De agora em diante, denote  $t = \rho^{-1}(l - 1)$ .

(3)  $\Rightarrow$  (1) É óbvio.

Vejamos (1)  $\Rightarrow$  (2). Suponhamos que para todo  $i \leq j < l$ ,  $x(\beta'')_w = R^u x(\eta'')_w$  e  $\lambda(\eta'') = 1 - \lambda(\beta'')$ , se  $d_{uw}$  é um único valor, ou  $\lambda(\eta'') = -\lambda(\beta'')$ , se  $d_{uw}$  é um conjunto. Pela hipótese de indução, as duas igualdades são equivalentes. Daí, temos que os 3 pontos

que geram os planos  $H_{\eta''}$  e  $H_{\beta''}$  pertencem a  $H_\alpha$  ou são reflexões entre si através de  $H_\alpha$ , o que implica  $H_{\eta''} = R^u H_{\beta''}$  é válida para todo  $j$ . Em particular, é verdade se escolhermos  $\eta'', \beta'' \in \mathcal{V}_{l-1}$ . Ainda pela hipótese de indução, de (1)  $\Rightarrow$  (3) temos que  $a_u \cdot a_t^0 = a_u \cdot a_t^1$ . Logo,  $a_t^0, a_t^1$  tem direção semelhante com relação a  $a_u$ . Portanto, se  $d_{uw}$  é um único valor, pela equação (2.6),  $\lambda(\eta) = 1 - \lambda(\beta)$  se, somente se,  $x(\beta)_v = R^u x(\eta)_v$ , e se  $d_{uw}$  é um conjunto, pela equação (5.2),  $\lambda(\eta) = -\lambda(\beta)$  se, somente se,  $x(\beta)_v = R^u x(\eta)_v$ .

Vejamos (2)  $\Rightarrow$  (3). Suponhamos que para todo  $i \leq j \leq l$ ,  $\lambda(\eta'') = 1 - \lambda(\beta'')$ , se  $d_{uw}$  é um único valor, ou  $\lambda(\eta'') = -\lambda(\beta'')$ , se  $d_{uw}$  é um conjunto de valores. Demonstramos na implicação anterior que para todo  $i \leq j \leq l$ ,  $x(\beta'')_w = R^u x(\eta'')_w$ . Resta demonstrar que  $a_u \cdot a_v^0 = a_u \cdot a_v^1$ , isto é, que o ângulo  $\theta_v^0$  e  $\theta_v^1$  formado por esses vetores tem o mesmo cosseno. Lembramos novamente que  $H_\eta = R^u H_\beta$ . Pela hipótese de indução, sabemos que os ângulos  $\theta_t^0, \theta_t^1$  formados por  $a_u$  e por  $a_t^0, a_t^1$ , respectivamente, possuem o mesmo cosseno. Com Probabilidade 1, os planos  $H_\eta, H_\beta$  não são paralelos, implicando que seus vetores normais não são idênticos. Portanto,  $\theta_t^0 = -\theta_t^1$ . Denotando por  $\theta^0, \theta^1$  os ângulos formados por  $a_t^0$  e  $a_v^0$  e por  $a_t^1$  e  $a_v^1$ , respectivamente, também temos que  $H_{\eta''} = R^u H_{\beta''}$ , onde  $\eta'', \beta'' \in \mathcal{V}_{l-1}$ . Consequentemente os vetores normais desses quatro planos são simétricos, o que implica que  $\theta^0 = -\theta^1$  ou  $\theta^0 = \pi - \theta^1$ . Pela definição de  $a_v^0$  e  $a_v^1$ , como os produtos escalares são positivos, temos  $-\frac{\pi}{2} \leq \theta^0, \theta^1 \leq \frac{\pi}{2}$ , implicando em,  $\theta^0 = -\theta^1$ . Portanto,  $\theta_v^0 = \theta_t^0 + \theta^0 = -\theta_t^1 - \theta^1 = -\theta_v^1$ , e, consequentemente,  $\cos \theta_v^0 = \cos(-\theta_v^1) = \cos \theta_v^1$ .  $\square$

A próxima proposição é uma generalização da Proposição 3.2.

**Proposição 5.2.** *Considere uma subárvore  $\mathcal{T}'$  de  $\mathcal{T}$ , consistindo de 5 níveis consecutivos  $i-4, \dots, i$ , onde  $i \geq 7$ , conectados a um único nó  $\eta$  e tal que todos os nós em todos os níveis são marcados por  $\boxplus$ . Seja  $u = \rho^{-1}(i-4)$ ,  $w = \rho^{-1}(i-3)$ ,  $t = \rho^{-1}(i-1)$  e  $v = \rho^{-1}(i)$ . Sendo  $p$  o número de nós folha de  $\mathcal{T}'$  e  $Y' = \{y^j | j \leq p\}$  o conjunto de realizações parciais de  $G$  nos tais nós folhas, temos que:*

1. *Se  $d_{ut}$  e  $d_{wv}$  são valores únicos, a Proposição 3.2 é válida.*
2. *Considere  $d_{ut}$  um conjunto de  $q$  valores e  $d_{wv}$  um único valor ou vice versa. Se  $p = 2^4 q$ , com probabilidade 1, existe um conjunto  $H^{uv} \subseteq \mathbb{R}_+$  com  $|H^{uv}| = 2q$ , tais que  $\|y_u^j - y_v^j\| \in H^{uv}$  para cada  $j \leq p$ .*
3. *Considere  $d_{ut}, d_{wv}$  conjuntos de  $q$  valores. Se  $p = 2^4 q^2$ , com probabilidade 1, existe um conjunto  $H^{uv} \subseteq \mathbb{R}_+$  com  $|H^{uv}| = 2q^2$ , tais que  $\|y_u^j - y_v^j\| \in H^{uv}$  para cada  $j \leq p$ .*

*Demonstração.* Somente duas arestas, nomeadas  $\{u, t\}$  e  $\{w, v\}$ , podem assumir um conjunto de distâncias na subárvore  $\mathcal{T}'$ . Se nenhuma das duas arestas assumir um conjunto de valores, estamos no caso da Proposição 3.2 e não temos nada a fazer. Se  $\{u, t\}$  assumir um conjunto de distâncias mas  $\{w, v\}$  não, então no nível de  $t$  temos  $2q$  vezes mais nós

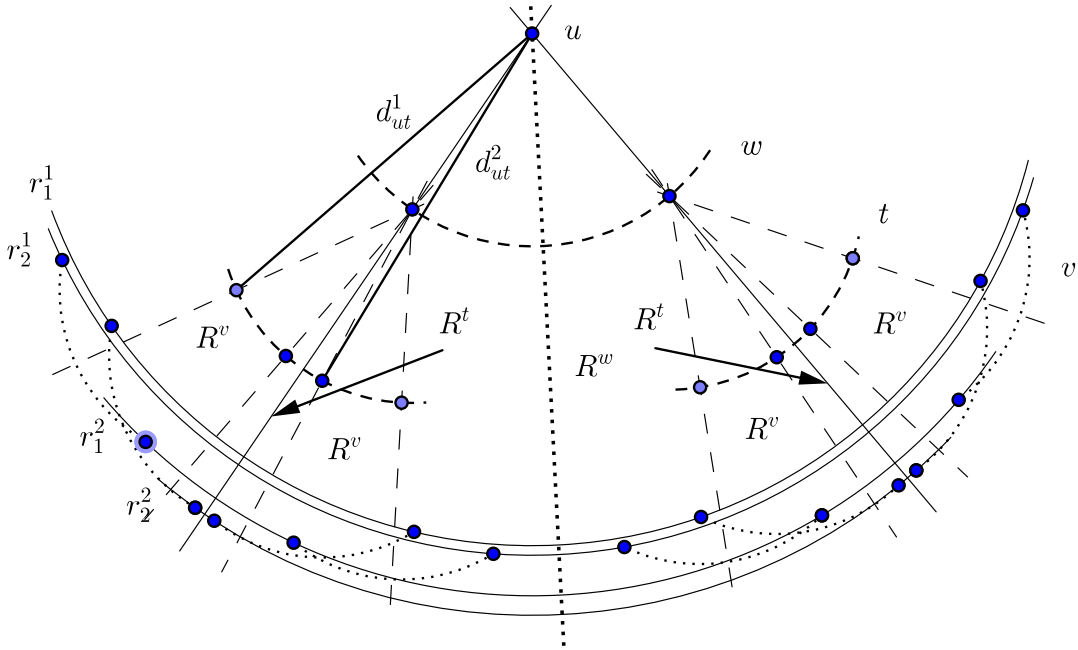


Figura 8 – Ilustração da Proposição 5.2 com  $K = 2$ ,  $d_{ut}$  com cardinalidade 2 e  $d_{wv}$  sendo um único valor.

que no nível anterior. Se  $\{w, v\}$  é um conjunto de distâncias mas  $\{u, t\}$  não é, então no nível  $v$  temos  $2q$  vezes mais nós que no nível  $t$ . Se ambos  $\{u, t\}, \{w, v\}$  são conjuntos de  $q$  distâncias, então em ambos os níveis o número de nós aumenta em  $2q$  vezes em relação ao anterior. Nos níveis  $s \in \{t, v\}$  que têm crescimento de  $2q$  vezes o número de nós com relação ao nível anterior cada par de nós  $\alpha^{1j}, \alpha^{2j}$ , onde  $\lambda(\alpha^{1j}) = -\lambda(\alpha^{2j})$  para  $j \leq p$ , é tal que  $x(\alpha^{1j})_s$  e  $x(\alpha^{2j})_s$  são reflexões, através de  $R^w$  pelo Lema 5.4. Assim, cada tal par gera uma subárvore de  $\mathcal{T}'$ , a qual, pela Proposição 3.2, com probabilidade 1, permite  $\|y_u^j - y_v^j\|$  apenas assumir valores em um conjunto  $S \subseteq \mathbb{R}_+$  com  $|S| = 2$ . Observe que qualquer par de tais conjuntos  $S$  tem interseção não-vazia, com probabilidade 0. Para o segundo caso, temos  $|H^{uv}| = 2q$  e, para o terceiro caso,  $|H^{uv}| = 2q^2$ , como queríamos demonstrar.  $\square$

Na Figura 8, ilustramos a Proposição 5.2, que é uma adaptação da Proposição 3.2 para o *iBP*. Consideramos  $K = 2$  com a cardinalidade de  $d_{ut}$  sendo dois e  $d_{wv}$  um valor único. Os arcos de círculos  $r_1^1, r_1^2, r_2^1, r_2^2$ , centrados em  $u$ , mostram as quatro possíveis distâncias entre a posição das realizações de  $u$  e  $v$ .

A seguir, apresentamos a generalização do resultado anterior para quando a diferença de níveis entre  $u$  e  $v$  é arbitrária.

**Corolário 5.2.** *Considere uma subárvore  $\mathcal{T}'$  de  $\mathcal{T}$ , consistindo de  $h+4$  níveis consecutivos  $i-h-3, \dots, i$ , onde  $i \geq 6+h$  e  $h \geq 1$ , conectados a um único nó  $\eta$ , tal que todos os nós de todos os níveis são marcados por  $\boxplus$ . Seja  $u = \rho^{-1}(i-h-3)$  e  $v = \rho^{-1}(i)$ ,  $p = 2^{h+3}q^r$ ,*

onde  $r$  é o número de vértices  $t$  entre  $u$  e  $v$ , tais que  $d_{t-3,t}$  é um conjunto de  $q$  valores reais positivos distintos. Considere o conjunto  $Y' = \{y_j | j \leq p\}$  de realizações parciais de  $G$  nos nós folhas de  $\mathcal{T}'$ . Então, com probabilidade 1, existe um conjunto  $H^{uv} = \{r_j | j \leq 2^h q^r\}$  de  $2^h q^r$  reais positivos distintos tais que  $\|y_u^j - y_v^j\| \in H^{uv} \forall j \leq p$ .

*Demonstração.* Para cada um dos vértices  $t_1, \dots, t_r$ , tais que  $d_{t_i-3,t_i}$   $i \leq r$  é um conjunto de  $q$  valores, o número de nós em relação ao vértice anterior aumenta em  $2q$ . Em cada nível  $s \in \{t_1, \dots, t_r\}$ , onde existe o crescimento de  $2q$  nós com relação ao nível anterior, cada par de nós  $\alpha^{1j}, \alpha^{2j}$  com  $\lambda(\alpha^{1j}) = -\lambda(\alpha^{2j})$   $j \leq p$  é tal que  $x(\alpha^{1j})$  e  $x(\alpha^{2j})$  são reflexões entre si. Assim, para cada tais pares, gera-se uma subárvore de  $\mathcal{T}'$ , a qual, pelo Corolário 3.2, com probabilidade 1, permite para  $\|y_u^j - y_v^j\|$  apenas valores em um conjunto  $S \subseteq \mathbb{R}_+$  tal que  $|S| = 2^h$ . Observe que qualquer par de tais conjuntos  $S$  tem interseção não-vazia, com probabilidade 0. Assim, como temos no máximo  $q^r$  ramificações geradas pelas distâncias dadas por conjuntos, segue que  $|H^{uv}| = 2^h q^r$ , implicando o resultado.  $\square$

Os Corolários 3.3 e 3.4 não mudam. Apesar da generalização do Teorema 3.1 possuir o mesmo enunciado, são necessárias algumas mudanças em sua demonstração. Desse modo, vamos enunciá-lo novamente e apresentar a demonstração com as mudanças.

**Teorema 5.1.** *Seja  $y \in X$  e  $v \in V - V_0$ , com  $\Upsilon(y, v)$  válido. Então, com probabilidade 1,  $\tilde{R}^v y \in X$ .*

*Demonstração.* Precisamos mostrar que  $\tilde{R}^v y$  é uma realização válida de  $G$ . Iniciamos particionando o conjunto  $E$  em 3 subconjuntos:  $E_1, E_2, E_3$ , onde  $E_1 = \{\{t, u\} \in E | t, u < v\}$ ,  $E_2 = \{\{t, u\} \in E | t, u \geq v\}$  e  $\{\{t, u\} \in E | t < v \wedge u \geq v\}$ . Para  $E_1$ , temos pela definição de  $\tilde{R}^v$  que  $\|(\tilde{R}^v y)_t - (\tilde{R}^v y)_u\| = \|Iy_t - Iy_u\| = \|y_t - y_u\| = d_{tu}$ . Para  $E_2$ , utilizamos a definição de  $\tilde{R}^v$  e o fato de  $R^v$  ser uma isometria, temos:  $\|(\tilde{R}^v y)_t - (\tilde{R}^v y)_u\| = \|R^v y_t - R^v y_u\| = \|y_t - y_u\| = d_{tu}$ . Para  $E_3$ , devemos mostrar que  $\|Iy_t - R^v y_u\| = d_{tu}$ . Como  $y \in X$ , pelo Lema 2.4, existe um nó folha factível  $\alpha$ , com  $x(\alpha) = y$ . Como  $\Upsilon(y, v)$  é válido, existe  $\eta \in \mathcal{V}_{\rho(v)-1}$  tal que  $x(\eta) = y[\gamma(v)]$  e  $\mu(\beta) = \boxplus$ , para todo  $\beta \in N^+(\eta)$ . Seja  $p(\alpha) \cap \mathcal{V}_{\rho(v)} = \{\beta\}$ , para algum  $\beta \in N^+(\eta)$ . Novamente, por  $\Upsilon(y, v)$ , existe pelo menos um nó folha factível  $\alpha'$ , tal que  $p(\alpha') \cap \mathcal{V}_{\rho(v)} = \{\beta'\}$  para algum  $\beta' \in N^+(\eta) - \{\beta\}$ . Sejam  $\{w\} = p(\alpha) \cap \mathcal{V}_{\rho(u)}$  e  $\{w'\} = p(\alpha') \cap \mathcal{V}_{\rho(u)}$ . Como  $w'$  é factível,  $\|x(w')_t - x(w')_u\| = d_{tu}$ . Como  $\eta$  é um antecessor de ambos  $\alpha$  e  $\alpha'$  no nível  $\rho(v) - 1$  e  $t < v$ ,  $p(\alpha') \cap \mathcal{V}_{\rho(t)} = p(\alpha) \cap \mathcal{V}_{\rho(t)}$ , o que implica que  $x(w')_t = x(w)_t = y_t$ . Assim,  $\|y_t - y_u\| = d_{tu} = \|y_t - x(w')_u\|$ . Além disso, como  $\beta' \in p(w') \cap \mathcal{V}_{\rho(v)}$ ,  $x(w')$  estende  $x(\beta')$ . Pela adaptação do algoritmo BP,  $\lambda(\beta) = 1 - \lambda(\beta')$ , se  $d_{u'-3,u'}$  é um único valor, e  $\lambda(\beta) = -\lambda(\beta')$ , se  $d_{u'-3,u'}$  é um conjunto de  $q$  valores. Como  $\alpha$  é factível em cada vértice  $u' \in V$ , tal que  $\rho(v) \leq \rho(u') \leq \rho(u)$ , o nó  $\theta \in p(\alpha) \cap \mathcal{V}_{\rho(u')}$  possui  $f \in \{1, 2\}$  subnós factíveis, se  $d_{u'-3,u'}$  é um único valor, ou  $f \in \{1, 2q\}$ , se  $d_{u'-3,u'}$  é um conjunto de  $q$  valores. No caso em que  $d_{u'-3,u'}$  é um único valor, pela Proposição



5.1, o nó  $\theta' \in p(\alpha') \cap \mathcal{V}_{\rho(u')}$  possui  $f$  subnós factíveis, se  $f = 2$ . Pelo Corolário 3.4 e Lema 5.4, podemos escolher  $\alpha'$  de forma que, com probabilidade 1,  $\lambda(\theta') = 1 - \lambda(\theta)$ . Se  $f = 1$ , pela adaptação do algoritmo BP, todos os nós mantêm ou trocam valor de  $\lambda$  dos seus antecessores, implicando em  $\lambda(\theta') = 1 - \lambda(\theta)$ . Assim, para este caso, segue do Lema 5.4, com probabilidade 1, que  $x(w')_u = R^v y_u$ , resultando em  $\|y_t - R^v y_u\| = d_{ut}$ . O caso em que  $d_{u'-3,u'}$  é um conjunto de  $q$  valores, se  $f = 2q$ , então, pelo Corolário 3.4 e Lema 5.4, podemos escolher  $\alpha'$  de forma que, com probabilidade 1,  $\lambda(\theta') = -\lambda(\theta)$ . Se  $f = 1$ , pela adaptação do algoritmo BP, todos os nós mantêm ou trocam valor de  $\lambda$  dos seus antecessores. Assim,  $\lambda(\theta') = -\lambda(\theta)$ . Neste caso, também segue do Lema 5.4, com probabilidade 1, que  $x(w')_u = R^v y_u$ , resultando em  $\|y_t - R^v y_u\| = d_{ut}$ , como queríamos demonstrar.  $\square$

### 5.3 O Número de Soluções

Como o espaço de busca do **iBP** ramifica em alguns níveis para  $2q$  possibilidades, segue que em geral o número de realizações possíveis não é mais uma potência de 2, mas sim um número da forma  $2^l q^K$ , para alguns inteiros  $l, K$ . Por este motivo, não vamos tentar generalizar os resultados do Capítulo 4 para a definição do algoritmo iBP. Vamos propor, então, um desenvolvimento um pouco diferente.

Definimos para todo  $v \in V$ ,  $\phi_v = \{0\}$ , se  $v \leq 3$ ,  $\phi_v = \{0, 1\}$ , se  $v > 3$  e  $d_{v-3,v}$  é um único valor e  $\phi_v = \{0, 1, \dots, 2q - 1\}$ , se  $v > 3$  e  $d_{v-3,v}$  é um conjunto de  $q$  valores. Seguimos definindo  $\chi$  com o objetivo de mapear as realizações em  $X$  por sequências indexadas por  $V$ , de tal forma que  $\chi_v \in \phi_v$ , para todo  $v \in V$ .

**Definição 5.1.** *Seja  $\alpha$  um nó da árvore iBP tal que  $x(\alpha)_v = y_v$ . Definimos a relação  $\chi_v = \lambda(\alpha)$ , se  $d_{v-3,v}$  é um único valor,  $\chi_v = \lambda(\alpha) - 1$ , se  $d_{v-3,v}$  é um conjunto e  $\lambda(\alpha) > 0$ , e  $\chi_v = q - \lambda(\alpha) - 1$ , se  $d_{v-3,v}$  é um conjunto e  $\lambda(\alpha) < 0$ .*

**Proposição 5.3.** *Com probabilidade 1, a relação  $\chi : X \rightarrow \{0, \dots, 2q - 1\}^n$  está bem definida.*

*Demonstração.* Temos que  $\chi$  não é bem definida, quando dados duas sequências distintas  $\chi^1, \chi^2$  em  $\{0, \dots, 2q - 1\}$  são associadas a uma única realização  $x \in X$ . Isto ocorre quando duas soluções dos sistemas quadráticos (5.1), na demonstração do Lema 5.1, são iguais, evento que ocorre com probabilidade 0. Portanto, com probabilidade 1,  $\chi$  está bem definida.  $\square$

Considere agora o conjunto  $\Xi = \{\chi(y) | y \in X\}$ . Vamos mostrar que este conjunto, munido da operação de adição módulo  $|\chi_v|$ , denotada por  $\oplus$ , é um grupo abeliano.



**Proposição 5.4.** *Com probabilidade 1,  $\Xi$  com a operação  $\chi^1 \oplus \chi^2 = (\chi_v^1 \oplus \chi_v^2 | v \in V)$ , onde  $\oplus$  denota a adição módulo  $|\phi_v|$ , é um grupo abeliano.*

*Demonstração.* Sejam  $\chi^1, \chi^2, \chi^3 \in \Xi$ . Inicialmente, vamos verificar a propriedade do fechamento, isto é, se  $\chi^1, \chi^2 \in \Xi$ , então  $\chi^1 \oplus \chi^2 \in \Xi$ . Como  $\chi^1, \chi^2 \in \Xi$ , existem  $y, y' \in X$  tais que  $\chi(y) = \chi^1$  e  $\chi(y') = \chi^2$ . Como  $\chi_i^1 \oplus \chi_i^2 \leq |\phi_i| - 1$ , pela Proposição 5.1, existe  $y'' \in X$  tal que para todo  $i \leq n$ ,  $\chi(y'')_i = \chi_i^1 \oplus \chi_i^2$ . Assim, segue que  $\chi^1 \oplus \chi^2 \in \Xi$ . Agora, vamos verificar a propriedade associativa:

$$\begin{aligned} \chi^1 \oplus (\chi^2 \oplus \chi^3) &= (\chi_1^1, \dots, \chi_n^1) \oplus (\chi_1^2 \oplus \chi_1^3, \dots, \chi_n^2 \oplus \chi_n^3) \\ &= (\chi_1^1 \oplus (\chi_1^2 \oplus \chi_1^3), \dots, \chi_n^1 \oplus (\chi_n^2 \oplus \chi_n^3)) \\ &= ((\chi_1^1 \oplus \chi_1^2) \oplus \chi_1^3, \dots, (\chi_n^1 \oplus \chi_n^2) \oplus \chi_n^3) \\ &= ((\chi_1^1 \oplus \chi_1^2, \dots, \chi_n^1 \oplus \chi_n^2) \oplus (\chi_1^3, \dots, \chi_n^3)) \\ &= (\chi^1 \oplus \chi^2) \oplus \chi^3. \end{aligned}$$

Continuamos com a verificação da propriedade comutativa:

$$\begin{aligned} \chi^1 \oplus \chi^2 &= (\chi_1^1 \oplus \chi_1^2, \dots, \chi_n^1 \oplus \chi_n^2) \\ &= (\chi_1^2 \oplus \chi_1^1, \dots, \chi_n^2 \oplus \chi_n^1) \\ &= \chi^2 \oplus \chi^1. \end{aligned}$$

Prosseguimos constatando que o elemento  $\chi^e = (0, \dots, 0) \in \Xi$  é o elemento neutro:

$$\begin{aligned} \chi^1 \oplus \chi^e &= (\chi_1^1 \oplus 0, \dots, \chi_n^1 \oplus 0) \\ &= (\chi_1^1, \dots, \chi_n^1) \\ &= \chi^1. \end{aligned}$$

Resta agora mostrar que, para qualquer elemento  $\chi^1 \in \Xi$ , existe um elemento  $\chi^{-1} \in \Xi$ , tal que  $\chi^1 \oplus \chi^{-1} = \chi^e$ . De fato,

$$\begin{aligned} \chi^1 \oplus \chi^{-1} = \chi^e &\Rightarrow (\chi_1^1 \oplus \chi_1^{-1}, \dots, \chi_n^1 \oplus \chi_n^{-1}) = (0, \dots, 0) \\ &\Rightarrow \chi_v^1 \oplus \chi_v^{-1} = 0 \pmod{|\phi_v|}, \forall v = 0, \dots, n \\ &\Rightarrow \chi_v^{-1} = (|\phi_v| - \chi_v^1) \pmod{|\phi_v|}, \forall v = 0, \dots, n \\ &\Rightarrow \chi^{-1} = ((|\phi_1| - \chi_1^1) \pmod{|\phi_1|}, \dots, (|\phi_n| - \chi_n^1) \pmod{|\phi_n|}). \end{aligned}$$

Para cada  $v \leq n$ ,  $(|\phi_v| - \chi_v^1) \pmod{|\phi_v|} < |\phi_v|$ , o que implica, pela Proposição 5.1, que  $\chi^{-1} \in \Xi$ . Portanto,  $\langle \Xi, \oplus \rangle$  é um grupo abeliano.  $\square$

A seguir, enunciamos alguns resultados técnicos com o intuito de obter ferramentas para a determinação da cardinalidade do conjunto solução  $X$ .

**Proposição 5.5.** *Com probabilidade 1, o grupo  $\langle \Xi, \oplus \rangle$  é subgrupo do grupo  $\bar{g} = \prod_{v \in V} C_{|\phi_v|}$ .*

*Demonstração.* Devemos mostrar que, dados  $\chi^1, \chi^2 \in \Xi$ , isto é, que existem  $x, x' \in X$  tais que  $\chi(x) = \chi^1, \chi(x') = \chi^2$  implica que  $\chi^1 \oplus (\chi^2)^{-1} \in \Xi$ . Temos que mostrar que existe uma realização  $x''$  em  $X$  tal que  $\chi(x'') = \chi^1 \oplus (\chi^2)^{-1}$ . Pelos Lemas 5.3 e 5.4, temos que existe uma realização  $y'$  tal que  $\chi(y') = (\chi^2)^{-1}$ . Agora, temos que  $\chi^1 \oplus \chi^2 = (\chi_1^1 \oplus \chi_1^2, \dots, \chi_n^1 \oplus \chi_n^2)$  para  $i \leq 3$ . Considerando  $x_i'' = x_i$  e como  $\chi_i^1 \oplus \chi_i^2 \leq |\phi_i| - 1$ , para todo  $i > 3$ , pela Proposição 5.1, temos que existe uma realização válida  $x''$  tal que  $\chi_i(x'') = \chi_i^1 \oplus (\chi_i^2)^{-1}$ . Logo,  $\chi(x'') = \chi^1 \oplus (\chi^2)^{-1}$ . Portanto,  $\langle \Xi, \oplus \rangle$  é subgrupo de  $\prod_{v \in V} C_{|\phi_v|}$ .  $\square$

**Proposição 5.6.** *O grupo  $\langle \Xi, \oplus \rangle$  age sobre si próprio.*

*Demonstração.* Defina

$$\begin{aligned} f : \langle \Xi, \oplus \rangle &\rightarrow \mathcal{P}(\Xi) \\ \chi &\rightarrow f_\chi, \end{aligned}$$

onde  $f_\chi : \Xi \rightarrow \Xi$  é definida como  $f_\chi(\chi') = \chi \oplus \chi'$ . Iniciamos verificando que  $f_\chi$  é injetora. Dados  $\chi', \chi'' \in \Xi$ , tais que  $f_\chi(\chi') = f_\chi(\chi'')$ , temos:

$$\begin{aligned} f_\chi(\chi') = f_\chi(\chi'') &\Rightarrow \chi \oplus \chi' = \chi \oplus \chi'' \\ &\Rightarrow \chi' = \chi'', \end{aligned}$$

implicando que  $f_\chi$  é injetora. Além disso, dado  $\chi' \in \Xi$ , tome  $\chi^{-1} \oplus \chi'$ . Temos, então:

$$f_\chi(\chi^{-1} \oplus \chi') = \chi \oplus (\chi^{-1} \oplus \chi') = (\chi \oplus \chi^{-1}) \oplus \chi' = \chi',$$

resultando que  $f_\chi$  é sobrejetora. Resta mostrar que  $f : \langle \Xi, \oplus \rangle \rightarrow \mathcal{P}(\Xi)$  é um homomorfismo. De fato:

$$\begin{aligned} f(\chi \oplus \chi') = f(\chi) \oplus f(\chi') &\Leftrightarrow f_{\chi \oplus \chi'}(\chi'') = (f_\chi \oplus f_{\chi'}) (\chi'') \\ &\Leftrightarrow (\chi \oplus \chi') \oplus \chi'' = \chi \oplus (\chi' \oplus \chi''), \end{aligned}$$

o que é válido pela propriedade associativa. Portanto,  $f$  é uma ação de  $\langle \Xi, \oplus \rangle$  no conjunto  $\Xi$ , como queríamos demonstrar.  $\square$

**Proposição 5.7.** *Para qualquer  $\chi \in \Xi$ , temos que  $\chi \oplus \Xi = \Xi$ .*

*Demonstração.* Vamos primeiro mostrar que  $\chi \oplus \Xi \subseteq \Xi$ . Se  $\chi' \in \chi \oplus \Xi$ , então  $\chi' = \chi \oplus \chi''$ , para algum  $\chi'' \in \Xi$ , e como  $\chi \in \Xi$ , então  $\chi \oplus \chi'' \in \Xi$ . Resta agora mostrar que  $\Xi \subseteq \chi \oplus \Xi$ . Se  $\chi' \in \Xi$ , temos que  $\chi \in \Xi$  e  $\chi^{-1} \in \Xi$ . Logo,  $\chi^{-1} \oplus \chi \in \Xi$ , implicando em  $\chi' = \chi \oplus (\chi^{-1} \oplus \chi') \in \Xi$ . Portanto,  $\chi \oplus \Xi = \Xi$ , como queríamos demonstrar.  $\square$

Considere  $v \in V$ , tal que  $\rho(v) > 3$ . Se  $d_{v-3,v}$  é um valor único, seja  $\iota_v = 1$ , e se  $d_{v-3,v}$  é um conjunto de  $q$  valores, seja  $\iota_v = q$ . Considere o conjunto  $\bar{\Lambda}$  com os seguintes elementos de  $\bar{g}$ :

- $\pi_v = (0, \dots, 0, \iota_v, \dots, \iota_n)$ , para todo  $v$  tal que  $\rho(v) > 3$ ;
- $\sigma_v = (0, \dots, 0, 1_v, 0, \dots, 0)$ , onde o 1 está na  $\rho(v)$  posição, para todo  $v$  tal que  $d_{v-3,v}$  é um conjunto.

**Proposição 5.8.** *O conjunto  $\bar{\Lambda}$  gera o grupo  $\bar{g}$ .*

*Demonstração.* Seja  $g \in \bar{g}$ . Devemos mostrar que  $g$  pode ser escrito como produto dos elementos pertencentes a  $\bar{\Lambda}$ . Temos que  $g = c_1 \cdots c_n$ , onde  $c_i \in C_{|\phi_i|} \forall i = 1, \dots, n$ , com  $|V| = n$ . Temos, então, que:

$$\begin{aligned} g &= c_1 \cdots c_n \\ &= (c_1, \dots, c_n). \end{aligned}$$

Como  $|\phi_1| = |\phi_2| = |\phi_3| = 1$ , então  $c_1 = c_2 = c_3 = 0$ , implicando em  $g = (0, 0, 0, c_4, \dots, c_n)$ . Além disso, para cada  $c_v$ ,  $v > 4$ , temos que  $c_v \sigma_v = (0, 0, 0, \dots, 0, c_v, 0, \dots, 0)$ . Também temos que  $\iota_v = 1$ , se  $d_{v-3,v}$  é um único valor, e  $\iota_v = q$ , se  $d_{v-3,v}$  é um conjunto de  $q$  valores. Isso implica em

$$(\iota_v + c_v) \mod |\phi_v| = c_v.$$

Logo, obtemos que

$$\begin{aligned} (0, 0, 0, c_4, \dots, c_n) &= (0, 0, 0, \iota_4 + c_4, \dots, \iota_n + c_n) \\ &= \pi_4 \oplus (0, 0, 0, c_4, \dots, c_n) \\ &= \pi_4 \oplus (c_4 \sigma_4) \oplus \dots \oplus (c_n \sigma_n). \end{aligned}$$

Portanto, o conjunto  $\bar{\Lambda}$  gera o grupo  $\bar{g}$ . □

Agora, estamos interessados em encontrar um subconjunto  $\Lambda$  de  $\bar{\Lambda}$ , que seja um conjunto gerador do grupo  $\langle \Xi, \oplus \rangle$ . Mais especificamente:

- Seja  $v \in V$ , tal que  $\rho(v) > 3$ . Se  $d_{v-3,v}$  é um único valor e para todos os nós do *iBP*, no nível  $v$  com dois subnós realizáveis, ambos os subnós possuem caminhos realizáveis até os nós folhas, então  $\pi_v \in \Lambda$ ;
- Seja  $v \in V$ , tal que  $\rho(v) > 3$ . Se  $d_{v-3,v}$  é um conjunto e para todos os nós do *iBP*, no nível  $v$  com  $2q$  subnós realizáveis, todos os nós possuem caminhos realizáveis até os nós folhas, então  $\pi_v, \sigma_v \in \Lambda$ .

**Teorema 5.2.** *Com probabilidade 1,  $\langle \Lambda, \oplus \rangle = \langle \Xi, \oplus \rangle$ .*

*Demonstração.* O fato de que  $\langle \Lambda, \oplus \rangle \subseteq \langle \Xi, \oplus \rangle$ , segue da definição, pois  $\pi_v$  representa um ramo válido no conjunto das realizações e os elementos  $\pi_v \oplus (\sigma_v \oplus \dots \oplus \sigma_v)$  representam

as  $2q$  ramificações nos casos em que temos um conjunto de  $q$  valores de distâncias para  $d_{v-3,v}$ . Assim,  $\langle \Lambda, \oplus \rangle \subseteq \langle \Xi, \oplus \rangle$ .

Resta agora mostrar que  $\langle \Xi, \oplus \rangle \subseteq \langle \Lambda, \oplus \rangle$ . Seja  $\chi'' \in \Xi$ . Procedemos por indução sobre os nós da realização  $\eta \in X$ , tal que  $\chi(\eta) = \chi''$ . Para  $n \leq 3$ , o resultado é válido, pois  $\chi''_n = 0$ . Assim, nosso processo de indução inicia com  $n = 4$ ; se  $d_{1,4}$  é um único valor, então temos  $\phi_4 = \{0, 1\}$ ; se  $\chi''_4 = 0$ , o resultado é válido e se  $\chi''_4 = 1$ , então considere  $\pi_4$  e o resultado segue. Se  $d_{1,4}$  é um conjunto com  $q$  valores, então  $\phi_4 = \{0, 1, \dots, 2q - 1\}$ ; se  $\chi''_4 = 0$ , o resultado é válido e se  $0 < \chi''_4 = t < q$ , tome  $\sigma_4^t$  e o resultado segue; se  $\chi''_4 = t \geq q$ , considere  $\pi_4 \oplus \sigma_4^{t-q}$  e daí o resultado é também válido. Se  $n > 4$ ,  $\forall j \in \{4, \dots, n-1\}$ , defina  $\Xi^j = \{\chi^j | \chi \in \Xi\}$  e  $\Lambda^j = \{\pi_l | l \leq j\}$ . Se no nível  $l$  temos dois subnós factíveis. Defina  $\Xi^j = \{\chi^j | \chi \in \Xi\}$  e  $\Lambda^j = \{\pi_l^k \oplus \sigma_l^h | k \in \{0, 1\} \wedge 0 \leq h \leq q-1, l \leq j\}$ . Se no nível  $l$  temos  $q$  subnós factíveis. Pela hipótese de indução, temos que  $\forall \chi' \in \Xi^j$ ,  $\chi' = \pi_j^{k'} \oplus \sigma_j^{h'}$  para algum  $k' \in \{0, 1\}$  e  $0 \leq h' \leq q-1$ . Agora, se  $d_{n-3,n}$  é um único valor, pela Proposição 2.1, com probabilidade 1, se existe no nível  $n$  pelo menos uma distância de poda, então  $\mathcal{V}_{n-1}$  possui 0 ou 1 subnós factíveis. Seja  $B_1^n$  o conjunto de todos tais subnós factíveis. Se no nível  $n$  não existem distâncias de poda, então  $\mathcal{V}_{n-1}$  tem 0 ou 2 subnós factíveis. Seja  $B_2^n$  o conjunto de todos tais subnós factíveis. No primeiro caso, seja  $\Xi^n = \{\chi(x(\beta)) | \beta \in B_1^n\}$  e  $\Lambda^n = \Lambda^{n-1}$ . Segue pela hipótese de indução que o resultado é válido. No segundo caso, seja  $\Xi^n = \{\chi(x(\beta)) | \beta \in B_2^n\}$  e  $\Lambda^n = \Lambda^{n-1} \cup \{\pi_n\}$ , temos que  $\pi_n = (0, \dots, 1)$ . Então, dado  $\chi''$ , pela hipótese de indução e pela idempotência de  $\pi_n$ , temos que

$$\chi'' = \prod_{3 < j \leq n-1} (\pi_j^{k'} \oplus \sigma_j^{h'}) \oplus \pi_n^{k''},$$

onde  $k'' \in \{0, 1\}$ , implicando que o resultado é válido. Se temos que  $d_{n-3,n}$  é um conjunto de  $q$  valores, então, pela Proposição 5.1, com probabilidade 1, se existe no nível  $n$ , pelo menos, uma distância de poda, então  $\mathcal{V}_{n-1}$  possui 0 ou 1 subnós factíveis. Seja  $B_1^n$  o conjunto de todos tais subnós factíveis. Se no nível  $n$  não existem distâncias de poda, então  $\mathcal{V}_{n-1}$  possui 0 ou  $2q$  subnós factíveis. Seja  $B_q^n$  o conjunto de todos tais subnós factíveis. No primeiro caso, seja  $\Xi^n = \{\chi(x(\beta)) | \beta \in B_1^n\}$  e  $\Lambda^n = \Lambda^{n-1}$ . Segue da hipótese de indução que o resultado é válido. No segundo caso, seja  $\Xi^n = \{\chi(x(\beta)) | \beta \in B_q^n\}$  e  $\Lambda^n = \Lambda^{n-1} \cup \{\pi_n, \sigma_n\}$ . Temos então que  $\pi_n = (0, \dots, q)$  e  $\sigma_n = (0, \dots, 1)$ . Portanto, dado  $\chi'' \in \Xi$ , pela hipótese de indução e pela idempotência de  $\pi_n$ , temos que

$$\chi'' = \prod_{3 < j \leq n-1} (\pi_j^{k'} \oplus \sigma_j^{h'}) \oplus (\pi_n^{k''} \oplus \sigma_n^{h''}),$$

onde  $k'' \in \{0, 1\}$  e  $0 \leq h'' \leq q-1$ , implicando que  $\langle \Xi, \oplus \rangle \subseteq \langle \Lambda, \oplus \rangle$ . Portanto,  $\langle \Xi, \oplus \rangle = \langle \Lambda, \oplus \rangle$ , como queríamos demonstrar.  $\square$

O Teorema 5.2 garante que, possuindo uma única realização  $x \in X$  e conhecendo o grupo de operadores de reflexões parciais  $\langle \Xi, \oplus \rangle$ , é possível encontrar todo o conjunto de realizações  $X$ . Nosso próximo objetivo é estimar o número de possíveis realizações em  $X$ .

**Proposição 5.9.** *Seja  $M$  o número de vértices  $v$ , com  $\rho(v) > 3$ , tais que  $d_{v-3,v}$  é um conjunto. Então,  $|\langle \Lambda, \oplus \rangle| \leq 2^l q^k$ , onde  $l \leq n - 3$  e  $k \leq M$ .*

*Demonstração.* Provaremos este resultado analisando o caso em que o máximo de distintas realizações dos nós ocorre em cada nível. Os 3 primeiros vértices são fixos, gerando uma única possibilidade. Para os  $M$  vértices  $v$ , onde  $d_{v-3,v}$  é um conjunto de  $q$  valores, obtemos no máximo um total de  $2^M q^M$  possibilidades de realizações, restando ainda  $n - M - 3$  vértices para serem realizados, onde cada um deles possui no máximo 2 possíveis realizações. Assim, segue que

$$|\langle \Lambda, \oplus \rangle| \leq 2^M q^M 2^{n-3-M} \leq 2^{n-3} q^M.$$

□

Segue do Teorema 5.2, com probabilidade 1, que o grupo  $\langle \Xi, \oplus \rangle$  tem a mesma cardinalidade de  $\langle \Lambda, \oplus \rangle$  e, pela Proposição 5.7, segue que o conjunto  $\Xi$  possui a mesma cardinalidade, o que implica que o conjunto de realizações também possui esta cardinalidade.

### 5.3.1 Poda por Intervalos

Nesta seção, estamos interessados em analisar a cardinalidade do conjunto  $X$  quando utilizamos arestas de poda cujas distâncias são dadas por intervalos.

Se  $z \in \mathbb{R}^3$  é um candidato à localização da realização para o vértice  $v$  e  $u$  é um antecessor não imediato de  $v$ , isto é,  $u$  é um antecessor que satisfaz  $\rho(u) < \rho(v) - 3$ , então  $d_{uv}$  pode assumir como valores o intervalo  $[d_{uv}^L, d_{uv}^U]$ , ocasionando uma mudança no Algoritmo BP. Basicamente, o teste na linha 19 é dado por  $\|x(\beta)_u - z\| \notin [d_{uv}^L, d_{uv}^U]$ .

Pelos resultados obtidos na Proposição 3.2, Corolário 3.2, Proposição 5.2 e Corolário 5.2, garantimos que para  $u, v \in V$ , tais que  $\rho(v) - \rho(u) > 3$ , existe um conjunto  $H^{uv} \subseteq \mathbb{R}_+$  com um número par de valores possíveis que  $\|y_u - y_v\|$  pode assumir para qualquer  $y \in X$ . Além disso, com probabilidade 1, para qualquer valor  $r \in H^{uv}$  e realização parcial  $(y_1, \dots, y_u)$ , existem duas possíveis extensões  $y, y'$  para uma realização parcial sobre  $G[\gamma(v) \cup \{v\}]$ , tal que  $\|y_u - y_v\| = r$ . Também verificamos nos resultados dos Corolários 3.1 e 5.1 que temos  $y_w = R^{u+1} y'_w$ , para todo  $w \in V$  tal que  $\rho(u) < \rho(w) < \rho(v)$ . Além disso, pelos resultados apresentados no Capítulo 3, se tivermos um única aresta  $\{u, v\} \in E$ , com  $\rho(u) < \rho(v) - 3$  tal que  $d_{uv} = r$ , então esta aresta realiza a poda de todas as outras realizações, exceto para as duas que satisfazem  $\|y_u - y_v\| = r$ .

No caso em que temos  $d_{uv}$  dado por um intervalo, pode ocorrer o fato de este intervalo conter vários valores consecutivos de  $H^{uv}$  ou até mesmo conter o conjunto  $H^{uv}$  inteiro, podendo haver a poda de um número par de realizações para  $v$ , incluindo o zero.

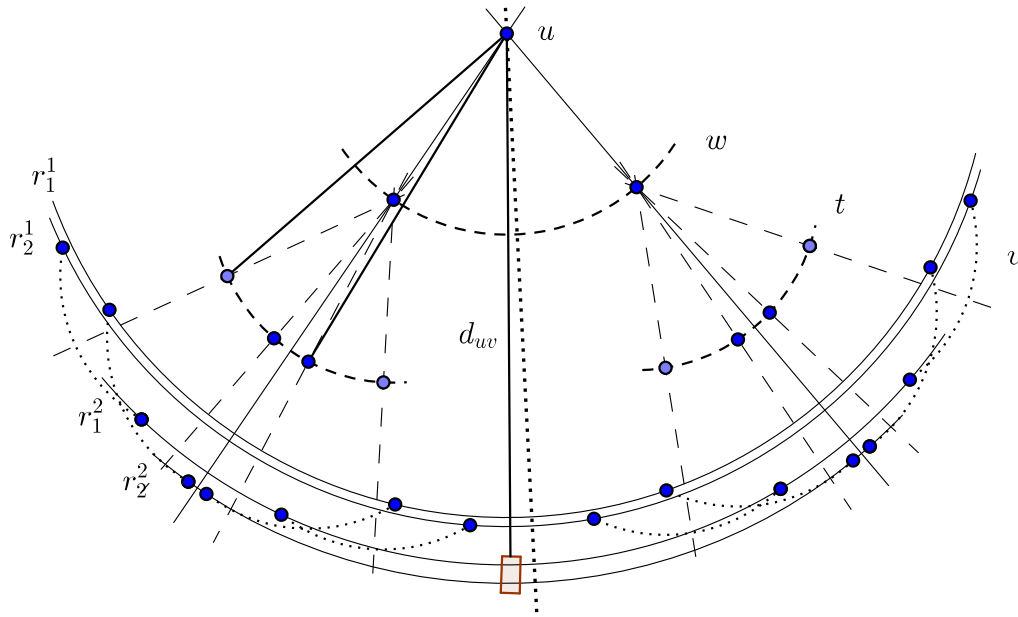


Figura 9 – Ilustração da utilização de distância intervalar para realizar podas na árvore de busca.

Portanto, é realmente difícil estimar a cardinalidade do conjunto  $X$  na situação de uma dada instância neste caso. Assumindo uma instância realizável, um dos resultados obtido, na Subseção 5.3, garante um limite inferior para este número e, obviamente, a cardinalidade do grupo  $\bar{g}$  garante um limite superior. Assim, existem  $l \leq n - 3$  e  $k \leq M$ , que dependem dos vértices  $u$  adjacentes a  $v$ , onde  $\rho(u) < \rho(v) - 3$ , tais que:

$$2^l q^k \leq |x| \leq 2^{n-3} q^M.$$

Na Figura 9, ilustramos a utilização de distâncias intervalares para a realização de podas no espaço de busca. Nesta ilustração, observamos que a distâncias intervalar  $d_{uv}$  permite somente 2 valores para  $H^{uv}$ , ao invés dos 4 inicialmente possíveis, sendo eles  $r_1^2, r_2^2$ . Consequentemente, o número de possíveis realizações do vértice  $v$  diminui de 16 para 8.

## 6 Considerações Finais

Neste trabalho, estudamos o Problema Discretizável de Geometria de Distâncias Moleculares (PDGDM), que é uma versão discreta do principal problema da Geometria de Distâncias, em que o espaço de busca pode ser representado por uma árvore binária e explorado por um algoritmo chamado Branch-and-Prune (BP).

Na árvore associada ao PDGDM, existem simetrias que podem tornar o método BP mais eficiente e fornecer informações sobre a quantidade de soluções do problema. Além da beleza teórica envolvida, esses resultados podem ser importantes nas aplicações do PDGDM, principalmente quando relacionadas a problemas de cálculo de estruturas tridimensionais de moléculas de proteínas.

Em problemas relacionados à estrutura de proteínas, os dados de distâncias são provenientes de experimentos de ressonância magnética nuclear (RMN). Nesse caso, o PDGDM deve ser modificado para poder se adaptar às características do problema real, onde os valores de algumas distâncias deixam de ser exatos, por conta das incertezas envolvidas nos experimentos de RMN. No último capítulo, estendemos os resultados que consideram distâncias exatas, já conhecidos na literatura, para tratar o caso com incertezas.

O prosseguimento natural deste trabalho está relacionado à extensão dos resultados apresentados para uma classe mais geral de problemas discretizáveis, o  $PDGD_3$ , onde se destacam o estudo de simetrias e a incorporação de incertezas nos dados do problema.

# Referências

- BRADY, T.; WATT, C. On products of euclidean reflections. *American Mathematical Monthly*, v. 113, n. 1, p. 826–829, 2006.
- COOPE, I. Reliable computation of the points of intersection of  $n$  spheres in  $\mathbb{R}^n$ . *The Australian and New Zealand Industrial and Applied Mathematics Journal*, v. 42, p. 461–477, 2000.
- CRIPPEN, G.; HAVEL, T. *Distance Geometry and Molecular Conformation*. New York: Wiley, 1988.
- GARCIA, A.; LEQUAIN, Y. *Elementos de álgebra*. 5th. ed. Rio de Janeiro: Impa, 2008.
- HERSTEIN, I. N. *Topics In Algebra*. 2nd. ed. New York: John Wiley & Sons, 1975.
- LAVOR, C.; LIBERTI, L.; MUCHERINO, A. The interval branch-and-prune algorithm for the discretizable molecular distance geometry problem with inexact distances. *Journal of Global Optimization*, v. 56, n. 3, p. 855–871, 2013.
- LIBERT, L.; LAVOR, C.; MUCHERINO, A. The discretizable molecular distance geometry problem seems easier on proteins. *Distance Geometry: Theory, Methods, and Applications*, Springer, New York, p. 47–60, 2013.
- LIBERTI, L.; LAVOR, C.; MACULAN, N. A branch-and-prune algorithm for the molecular distance geometry problem. *International Transactions in Operational*, v. 15, p. 1–17, 2008.
- LIBERTI, L.; LAVOR, C.; MACULAN, N.; MUCHERINO, A. Euclidean distance geometry and applications. *Siam Review*, SIAM, v. 56, n. 1, p. 3–69, 2014.
- LIBERTI, L.; MASSOM, B.; LEE, J.; LAVOR, C.; MUCHERINO, A. On the number of realizations of certain henneberg graphs arising in protein conformation. *Discrete Applied Mathematics*, Elsevier, v. 165, p. 213–232, 2014.