UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

MARCOS MERCANDELI RODRIGUES

INDEFINIBILIDADE DA REPRESENTABILIDADE DE MATROIDES EM LINGUAGENS MONÁDICAS DE SEGUNDA ORDEM

VITÓRIA
2022

MARCOS MERCANDELI RODRIGUES

INDEFINIBILIDADE DA REPRESENTABILIDADE DE MATROIDES EM LINGUAGENS MONÁDICAS DE SEGUNDA ORDEM

Dissertação de mestrado apresentada ao PPGMAT-Ufes como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática.

ORIENTADOR: Prof. Dr. João Paulo Costalonga

VITÓRIA
2022

Ficha catalográfica disponibilizada pelo Sistema Integrado de Bibliotecas - SIBI/UFES e elaborada pelo autor

---

Rodrigues, Marcos, 1993-
R696i Indefinibilidade da representabilidade de matroides em linguagens monádicas de segunda ordem / Marcos Rodrigues. - 2022.
117 f. : il.

Orientador: João Paulo Costalonga.
Dissertação (Mestrado em Matemática) - Universidade Federal do Espírito Santo, Centro de Ciências Exatas.

1. Matróides. 2. Lógica simbólica e matemática. 3. Matemática. I. Costalonga, João Paulo. II. Universidade Federal do Espírito Santo. Centro de Ciências Exatas. III. Título.

CDU: 51

Indefinibilidade da Representabilidade de Matroides em Linguagens Monádicas de Segunda Ordem

Marcos Mercandeli Rodrigues

Dissertação submetida ao Programa de Pós-Graduação em Matemática da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do grau de Mestre em Matemática.

Aprovada em 11 de abril de 2022 por:

Prof. Dr. João Paulo Costalonga
Universidade Federal do Espírito Santo
Orientador

Prof. Dr. Renan Maneli Mezabarba
Universidade Federal do Espírito Santo

Prof. Dr. Eudes Naziazeno Galvão
Universidade Federal de Pernanmbuco

Universidade Federal do Espírito Santo
Vitória, Abril de 2022

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

PROTOCOLO DE ASSINATURA

O documento acima foi assinado digitalmente com senha eletrônica através do Protocolo Web, conforme Portaria UFES nº 1.269 de 30/08/2018, por
RENAN MANELI MEZABARBA - SIAPE 1031823
Departamento de Matemática - DM/CCE
Em 11/04/2022 às 14:22

Para verificar as assinaturas e visualizar o documento original acesse o link:
https://api.lepisma.ufes.br/arquivos-assinados/445000?tipoArquivo=O

Emitido em 12/04/2022

CERTIFICADO Nº 994/2022 - DM CCEN (11.59.05)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 12/04/2022 16:27)
EUDES NAZIAZENO GALVAO
PROFESSOR DO MAGISTERIO SUPERIOR
2499363

Para verificar a autenticidade deste documento entre em http://sipac.ufpe.br/documentos/ informando seu número: **994**, ano: **2022**, tipo: **CERTIFICADO**, data de emissão: **12/04/2022** e o código de verificação: **4aa6fe34d2**

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

PROTOCOLO DE ASSINATURA

O documento acima foi assinado digitalmente com senha eletrônica através do Protocolo Web, conforme Portaria UFES nº 1.269 de 30/08/2018, por
JOAO PAULO COSTALONGA - SIAPE 1661705
Departamento de Matemática - DM/CCE
Em 10/05/2022 às 13:33

Para verificar as assinaturas e visualizar o documento original acesse o link:
https://api.lepisma.ufes.br/arquivos-assinados/469170?tipoArquivo=O

Este trabalho é dedicado à minha família.

AGRADECIMENTOS

Agradeço à minha família e a todas as pessoas que contruibuíram com a minha caminhada até aqui, como por exemplo as pessoas que foram e que são minhas professoras e minhas amigas. Agradeço também aos membros da banca avaliadora da defesa desta dissertação por suas sugestões e contribuições que ajudaram a melhorar este trabalho. Em especial, agradeço ao meu orientador João Paulo Costalonga pela orientação em um tópico que relaciona Lógica Matemática e Teoria de Matroides. Por fim, agradeço à Coordenação de Aperfeiçoamento Pessoal de Nivel Superior (CAPES) pela concessão de bolsa de estudos e à Universidade Federal do Espírito Santo (Ufes) pela infraestrutura.

"*Eg var og eg er vind,*
Eg er vinda, vevja
Hapt og tvinna"
— Einar Selvik

RESUMO

Neste trabalho serão apresentados resultados importantes descobertos por D. Mayhew, M. Newman e G. Whittle nas áreas de Teoria de Matroides e Lógica Matemática, mais especificamente em Teoria de Modelos Finitos e Indefinibilidade. Mostraremos que certos tipos de linguagens monádicas de segunda ordem não são capazes de expressar as representabilidades linear e algébrica de matroides, sendo esta última uma extensão da primeira e uma contribuição do trabalho desenvolvido. Apresentaremos também uma classe de matroides estudada por T. Zaslavsky chamadas matroides de ganho e uma construção de matroides chamada de amálgama própria.

PALAVRAS–CHAVE:

Matroides,
Modelos Finitos,
Linguagem Monádica de Segunda Ordem,
Indefinibilidade,
Representabilidade de Matroides.

ABSTRACT

In this work we shall present important results on matroid theory and mathematical logic, more specifically in finite model theory and undefinability discovered by D. Mayhew, M. Newman, and G. Whittle. We shall prove that some monadic second-order languages cannot define linear and algebraic matroid representability, the latter being an extension of the former and a contribution of the development of this thesis. We shall also present a class of matroids studied by T. Zaslavsky called gain matroids and a matroid construction called proper amalgam.

KEY–WORDS:

Matroids,
Finite models,
Monadic second-order language,
Undefinability,
Matroid representability.

SUMÁRIO

I INTRODUÇÃO

Este trabalho tem como objetivo o estudo das indefinibilidades das representabilidades linear e algébrica de matroides em uma certa linguagem. Isto quer dizer que nós vamos mostrar que uma *linguagem formal*[a] específica não é capaz de expressar estas propriedades. Apresentaremos nos demais capítulos desta dissertação os conceitos básicos da Teoria de Matroides e de Linguagens Formais necessários para este fim. O público-alvo do texto são as pessoas de pós-graduação em Matemática ou Ciência da Computação e finalistas das graduações destas áreas que tenham interesse em Lógicas, Combinatória e Matemática Discreta. Não assumiremos que tal público-alvo tenha familiaridade com Teoria de Matroides ou com Lógicas, e portanto, os Capítulos II e III suprirão os requisitos necessários para que estas pessoas possam entender os resultados desta dissertação. Pessoas que já estão familiarizadas com os temas abordados não serão prejudicadas por isso e podem, caso queiram, seguir diretamente para a Seção III.5 do Capítulo III. Usaremos a expressão "sse" para abreviar "se, e somente se" ao longo do texto. Os símbolos mais usados na dissertação podem ser consultados na Lista de Símbolos.

A Teoria de Matroides[b] foi iniciada e fundamentada em 1935 pelos matemáticos T. Nakasawa e H. Whitney de maneira independente para formalizar uma noção de independência advinda de espaços vetoriais [9]. A axiomatização inicial apresentada por Nakasawa formaliza este conceito segundo um cálculo abstrato de ciclos [14], enquanto a axiomatização inicial apresentada por Whitney o formaliza segundo conjuntos independentes abstratos [9]. Estes dois sistemas axiomáticos capturam surpreendentemente o mesmo conceito de independência, apesar de sua patente distinção. Este fenômeno (chamado "criptomorfismo" [1]) não é exclusivo[c] da Teoria de Matroides, embora seja nesta teoria que tal fenômeno se mostre mais evidente: matroides podem ser descritas por certas coleções de conjuntos ou por certas funções, que satisfazem certos postulados descritos em alguma linguagem. Todas estas maneiras distintas de descrever uma matroide formalizam um mesmo conceito de independência que ocorre em Álgebra Linear, Teoria de Corpos, Geometria Projetiva, Teoria de Grafos, Teoria de Modelos e Computação. Estas ocorrências de matroides em contextos matemáticos tão distintos evidenciam a importância e a relevância deste tópico da Matemática Discreta.

Teorias matemáticas podem ser axiomatizadas em linguagens formais capazes de expressar seus axiomas. Diferentemente das linguagens naturais, linguagens formais são descritas por meio de regras gramaticais formais e esta artificialidade linguística introduz limitações sobre quais tipos de conceitos uma dada linguagem formal é capaz de expressar. Um exemplo clássico de tal fenômeno é a incapacidade de linguagens de primeira ordem de expressar finitude em virtude do

[a] O termo "formal" indica que a linguagem não é uma linguagem natural, i.e. não é uma linguagem como Português, Inglês, Alemão, dentre outras, que foram desenvolvidas por humanos levando em conta as particularidades geográficas, culturais, sociais e ambientais das regiões que habitam no presente ou que habitaram no passado. Em geral, uma linguagem formal é um conjunto de expressões construídas por meio de regras bem-definidas que transformam os símbolos básicos do alfabeto da linguagem. Este conceito vago de linguagem formal ficará claro no Capítulo III.

[b] Nesta dissertação o termo "matroide" será sinônimo do termo "matroide finita".

[c] E.g. o axioma $A \cup cl(A) \cup cl(cl(B)) = cl(A \cup B) - cl(\emptyset)$ em Topologia (Vide W. Pervin [16]).

Teorema da Compacidade: em outras palavras, a finitude não é uma propriedade de primeira ordem [20]. Este exemplo evidencia que a Teoria de Matroides exige uma linguagem de ordem superior para ser expressa. Apresentaremos um tipo específico de linguagem monádica de segunda ordem, como feito por D. Mayhew, M. Newman e G. Whittle [12], que é capaz de expressar os axiomas da Teoria de Matroides. O termo "segunda ordem" diz respeito à quantificação de segunda ordem sobre predicados, enquanto o adjetivo "monádica" diz respeito a restrição destes predicados aos predicados monádicos (entendemos "predicado monádico" como sinônimo de "conjunto de indivíduos"). Linguagens formais são acompanhadas de uma classe de estruturas matemáticas capazes de interpretar os seus símbolos constantes para que seja desenvolvida uma *semântica formal*[d]. Com a axiomatização da Teoria de Matroides na linguagem formal apresentada e uma semântica plena para linguagens monádicas de segunda ordem será possível estudar matroides do ponto de vista da Teoria de Modelos Finitos. Neste contexto, poderemos estudar a *teoria objeto*[e] segundo esta perspectiva. Nosso objetivo principal é estudar a indefinibilidade de certas classes de matroides nesta linguagem.

O Capítulo II apresentará os conceitos de Teoria de Matroides necessários para alcançar os objetivos principais deste trabalho. Nosso objetivo nesse capítulo é descrever e obter os resultados necessários sobre matroides para provar os resultados de indefinibilidade no Capítulo III. Na Seção II.1, apresentaremos as noções básicas de Teoria de Grafos que serão usadas para o estudo dos conceitos de Teoria de Matroides presentes neste trabalho. Na Seção II.2, apresentaremos a axiomatização da Teoria de Matroides em termos de conjuntos independentes, além dos conceitos clássicos de bases, circuitos, função posto e operador de fecho e como eles também caracterizam uma matroide. Finalizaremos a seção com a apresentação de matroides duais, que são importante para descrever *menores*[f] de uma matroide. Na Seção II.3, apresentaremos a noção de representabilidade linear de matroides e menores. Na Seção II.4 será apresentada a construção de amálgama própria de matroides e suas condições de existência. Esta seção será uma das mais importantes do capítulo, pois contém o Teorema II.4.13 que caracteriza os conjuntos independentes de um tipo especial de amálgama própria que é importante para obter os resultados sobre um método efetivo de decisão no Capítulo III. Finalizaremos o Capítulo II com a apresentação da Seção II.5, na qual serão discutidos resultados básicos sobre matroides de ganho e a construção de duas classes especiais deste tipo de matroide. Nesta seção, apresentaremos as classes de grafos de viés e de ganho que serão utilizadas para construir matroides de ganho. Apresentaremos também o Teorema II.5.3 e seu corolário, uma vez que eles serão bem úteis para esse fim. Os resultados mais importantes dessa última seção são o Teorema II.5.12, que evidencia sob quais condições uma matroide de ganho é linearmente representável e os Teoremas II.5.14 e II.5.15, que evidenciam sob quais condições certas amálgamas próprias de matroides de ganho específicas

[d]Uma vez estabelecida uma semântica formal, poderemos expressar de maneira clara o que quer dizer uma sentença da linguagem ser verdadeira (em uma estrutura). A noção de verdade estudada é formal no sentido de ser uma propriedade monádica de sentenças da linguagem e não de existir uma correspondência com os fatos materiais concretos no mundo em que vivemos.

[e]Em lógica é comum distinguir níveis de linguagem. Em um deles há a *linguagem objeto*, que é a linguagem estudada de maneira sistemática. Tal estudo sistemático também exige uma linguagem para ser feito, que é a *metalinguagem*: a linguagem sobre a linguagem. Neste sentido, a teoria objeto é a Teoria de Matroides expressa na linguagem formal que será apresentada.

[f]Em uma teoria matemática é comum descrever subestruturas de estruturas da teoria. O conceito de subestrutura em Teoria de Matroides é o de menor e ele será descrito na Seção II.2.

são linearmente representáveis.

O Capítulo III apresentará os conceitos de Lógica Monádica de Segunda Ordem necessários para alcançar os objetivos principais deste trabalho. Nosso objetivo nesse capítulo é obter os resultados sobre as indefinibilidades das representabilidades linear e algébrica. Começaremos o capítulo pela descrição da sintaxe e da semântica da linguagem monádica de segunda ordem eleita como linguagem paradigmática para axiomatizar a Teoria de Matroides em Lógica Monádica de Segunda Ordem. Na Seção III.1, apresentaremos as regras sintáticas de formação de fórmulas, de dedução lógica e de reescrita de fórmulas. As regras de dedução permitirão obter um sistema de dedução formal e uma noção de teorema. As regras de reescrita serão importantes para exibir o processo de construção de *formas normais prenex*[g] para fórmulas da linguagem objeto. Um resultado importante dessa seção é o Teorema III.1.11 e seus corolários que demonstram a corretude sintática de tal reescrita. Na Seção III.2, apresentaremos a semântica da linguagem objeto baseada no que é feito por D. van Dalen [20] e por J. Shoenfield [17] pelo emprego de *nomes*[h]. O Teorema III.2.3 demonstra a corretude do sistema de dedução apresentado na Seção III.1 e o restante da seção apresenta propriedades semânticas importantes da Teoria de Matroides em Lógica Monádica de Segunda Ordem[i]. Após apresentar estes conceitos básicos, dedicaremo-nos à demonstração dos resultados lógicos principais deste trabalho que dizem respeito à indefinibilidade. Na Seção III.5, vamos mostrar que a linguagem objeto estudada não é capaz de expressar a representabilidade linear de matroides. O Teorema III.3.8 será de extrema importância para alcançar esses resultados. Na Seção III.4, vamos mostrar que a linguagem introduzida na Seção III.1 não é capaz de expressar a representabilidade algébrica de matroides. A motivação desta extensão dos resultados de linear para álgébrico é bem natural: se uma matroide é linearmente representável, então ela é algebricamente representável. Seria particularmente estranho que uma linguagem pudesse definir a classe das matroides algebricamente representáveis, mas não a classe das matroides linearmente representáveis. Na Seção III.5, vamos mostrar que existe um método de decisão para determinar quais conjuntos são independentes em uma certa classe de amálgamas próprias de matroides. Finalizaremos o capítulo com a Seção III.6, na qual mostraremos que é possível obter outras linguagens que compartilham das limitações da linguagem introduzida na Seção III.1.

[g] Formas normais são formas que certas fórmulas da linguagem têm e que apresentam características que facilitam as análises e os estudos sistemáticos de certas propriedades da linguagem. A existência de uma fórmula em forma normal prenex para cada fórmula da linguagem objeto será muito útil para o desenvolvimento do estudo no que diz respeito à compatibilidade de um número de objetos que vamos definir ao longo do Capítulo III.

[h] Nomes serão úteis para estudar as interpretações das sentenças da linguagem objeto nas estruturas. Isso permite iniciar a semântica sem o emprego de funções que mapeiam variáveis em conjuntos de indivíduos das estruturas.

[i] Durante o processo de investigação sistemática da Teoria de Matroides em Lógica Monádica de Segunda Ordem, vamos obter resultados que dizem respeito à uma teoria matemática por meio da aplicação de ferramentas matemáticas sobre essa parte da própria matemática. Estamos diante de uma dualidade bem interessante, pois podemos ver o estudo matemático da própria matemática como um fenômeno tanto abstrato quanto aplicado.

II TEORIA DE MATROIDES

II.1 CONCEITOS BÁSICOS DE GRAFOS

Apresentaremos nesta seção conceitos básicos de Teoria de Grafos necessários para descrever grafos de ganho e grafos de viés, além dos conceitos de Teoria de Matroides do presente trabalho. Essas duas classes de grafos serão usadas para construir classes de matroides de ganho na Seção II.5 e essa construção dependerá dos resultados do Teorema II.5.3 e seu corolário. As referências principais desta seção são R. Diestel [2] e J. Oxley [15].

Um *grafo* é uma lista $G = (V(G), E(G), \Lambda_G)$, na qual $V(G)$ e $E(G)$ são conjuntos finitos e disjuntos de *vértices* e *arestas* de G, respectivamente, e Λ_G é uma função chamada *função de incidência* de G que associa cada aresta de G a um único par não-ordenado de vértices de G; dizemos, neste caso, que a aresta *incide* aos vértices deste único par não-ordenado. Duas arestas são *paralelas* quando incidem aos mesmos dois vértices. Um *loop* é uma aresta que incide a um único vértice e um grafo é *simples* quando não possui arestas paralelas e não possui loops. Uma *representação geométrica* de um grafo é uma função que associa seus vértices a pontos no plano e suas arestas a arcos no plano de modo a explicitar a sua função de incidência do seguinte modo: um arco é desenhado ligando dois pontos no plano sse a aresta correspondente ao arco incide aos vértices correspondentes aos pontos no grafo. A Figura II.1.1 ilustra uma tal representação. É comum identificar uma representação geométrica de um grafo com o próprio grafo em alguns contextos, pois isto permite descrevê-lo mais facilmente. Um *isomorfismo* de grafos é uma mudança de rotulação de vértices e arestas que preserva incidências. Mais formalmente, dizemos que dois grafos G e H são *isomorfos* e escrevemos $G \cong H$ quando existe uma bijeção de $V(G) \cup E(G)$ em $V(H) \cup E(H)$ que mapeia vértices em vértices e arestas em arestas de modo a preservar incidências. A Figura II.1.1 apresenta grafos isomorfos.

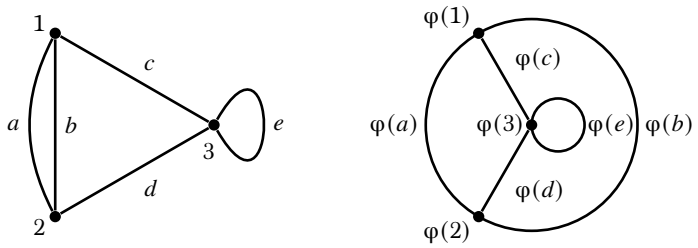

Figura II.1.1: Na figura são apresentados dois grafos cujos vértices e arestas estão rotulados pelos símbolos que acompanham pontos e arcos da representação geométrica. A função de incidência dos grafos da figura é informada pela configuração de pontos e arcos apresentada. Os dois grafos da figura são isomorfos e a correspondência $x \mapsto \varphi(x)$ determina um isomorfismo.

Dados dois grafos G e H, dizemos que H é um *subgrafo de* G e escrevemos $H \sqsubseteq G$ quando $V(H) \subseteq V(G)$ e $E(H) \subseteq E(G)$ e $\Lambda_H \subseteq \Lambda_G$. Observemos que em qualquer família de grafos a relação $\sqsubseteq$ é uma relação de ordem.

EXEMPLO II.1.1 (Grafos).

(1) O grafo *caminho* P_m de m vértices é um grafo simples que captura a noção intuitiva de caminho. O caminho nulo P_0 é o grafo sem vértices e arestas. O caminho trivial P_1 é o grafo com um único vértice e nenhuma aresta. Para $m \in \mathbb{N}$ com $1 < m$, definimos P_m da seguinte maneira: os vértices de P_m são $1, \ldots, m$, as arestas de P_m são $\{1, 2\}, \ldots, \{m-1, m\}$ e a função de incidência de P_m é a inclusão. Vale $|E(P_m)| = m - 1$ e grafos caminho são grafos simples. Um vértice no qual incide uma única aresta é chamado de extremidade do caminho. A Figura II.1.2 apresenta o grafo P_5.

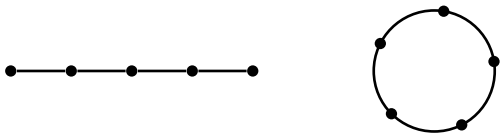

Figura II.1.2: Os grafos caminho P_5 do lado esquerdo e ciclo C_5 do lado direito.

(2) Suponhamos que $m \in \mathbb{N}$ seja positivo. O grafo *ciclo* C_m de m vértices é um grafo que captura a noção intuitiva de ciclo e ele é obtido de um grafo caminho P_m pela adição de uma nova aresta que incide às extremidades do caminho. Vale $|E(C_m)| = m$. A Figura II.1.2 apresenta o grafo C_5. Grafos ciclos são simples para $3 \leq m$. Se $H \sqsubseteq G$ tem m vértices e $H \cong C_m$, então dizemos que H é um *ciclo de* G e que E(H) é um *circuito de* G.

Figura II.1.3: O grafo completo K_5.

(3) O grafo *completo* K_m de m vértices é o grafo simples cujo número de arestas é o maior possível para este número de vértices. Vale $|E(K_m)| = m(m-1)/2$. Observemos que se G é um grafo simples de m vértices, então G é isomorfo a um subgrafo de K_m. A Figura II.1.3 apresenta o grafo K_5.

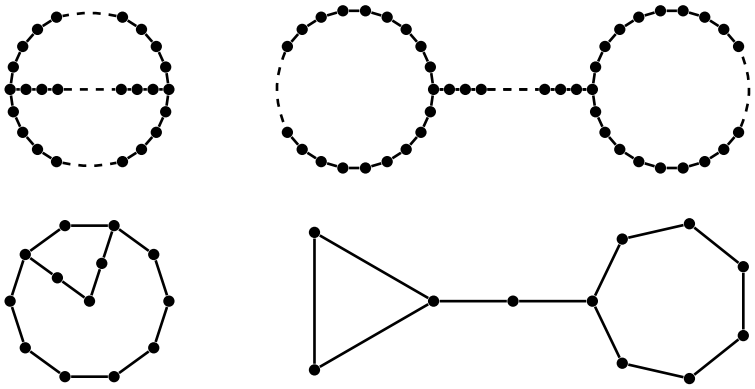

Figura II.1.4: Na parte superior, temos as formas gerais dos grafos theta do lado esquerdo e algema do lado direito. Na parte inferior, temos exemplos concretos de tais grafos.

(4) Um grafo theta é formado por três grafos caminho que compartilham exatamente as suas extremidades de acordo com o que mostra a Figura II.1.4. Um grafo *algema frouxa* é formado por dois grafos ciclo que não compartilham vértices e um grafo caminho que os conecta de acordo com o que mostra a Figura II.1.4. Um grafo *algema apertada* é formado por dois grafos ciclo que compartilham um único vértice. ⊣

Suponhamos que G seja um grafo. Dado $U \subseteq V(G)$, dizemos que $G[U]$ é o subgrafo de G *induzido* por U quando $V(G[U]) = U$ e $E(G[U])$ é o conjunto de todas as arestas de G que incidem somente aos vértices em U. Dado $F \subseteq E(G)$, dizemos que $G \mid F$ é o subgrafo de G *restrito* a F quando $V(G \mid F)$ é o conjunto de todos os vértices de G que incidem às arestas de F e $E(G \mid F) = F$. Dados $m \in \mathbb{N}$ positivo e $u, v \in V(G)$, um (u, v)-*passeio* de tamanho m em G é uma lista finita, não-vazia e alternada de vértices e arestas da forma

$$W(u, v) = v_1, e_1, v_2, \ldots, v_m, e_m, v_{m+1}$$

tal que $v_1 = u$ e $v_{m+1} = v$ e $\Lambda_G(e_i) = \{ v_i, v_{i+1} \}$ para cada $i \in \{1, \ldots, m\}$. Os vértices u e v são a origem e o destino do passeio, respectivamente. Dizemos que um (u, v)-passeio é *fechado* quando $u = v$. Um (u, v)-*caminho* de um grafo G é um (u, v)-passeio de G cujos vértices são todos distintos. O grafo G é *conexo* quando existe um (u, v)-caminho de G para quaisquer $u, v \in V(G)$. Cada subgrafo conexo $\sqsubseteq$-maximal de um grafo é chamado de *componente conexa* do grafo. Uma *floresta* é um grafo simples sem ciclos e uma *árvore* é uma floresta conexa. Dizemos que $H \sqsubseteq G$ é uma *floresta geradora* de um grafo G quando H é uma floresta $\sqsubseteq$-maximal e $G[V(H)] = G$. A Figura II.1.5 ilustra duas árvores geradoras do grafo de Petersen.

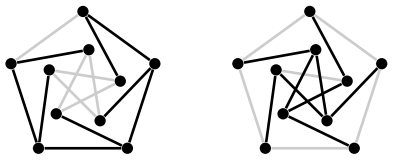

Figura II.1.5: Duas árvores geradoras do grafo de Petersen em destaque na figura.

II.2 MATROIDES

Apresentaremos nesta seção resultados básicos da Teoria de Matroides que serão relevantes para a descrição de amálgamas próprias, matroides de ganho e representabilidade linear de matroides. A referência principal desta seção é J. Oxley [15].

Dado um conjunto finito E, dizemos que $\mathcal{I} \subseteq 2^E$ é uma coleção *hereditária* quando $I \in \mathcal{I}$ sempre que $I \subseteq J$ e $J \in \mathcal{I}$. Dizemos também que $\mathcal{I}$ tem a *propriedade de aumento* quando $|I| < |J|$ é suficiente para que exista $a \in J - I$ tal que $I \cup a \in \mathcal{I}$[a], quaisquer que sejam $I, J \in \mathcal{I}$. Uma *matroide*[b] é um par $M = (E(M), \mathcal{I}(M))$, no qual $E(M)$ é um conjunto finito e $\mathcal{I}(M)$ é uma coleção não-vazia de subconjuntos de $E(M)$ que é hereditária e possui a propriedade de aumento[c]. Os elementos de $\mathcal{I}(M)$

[a] Vamos escrever $X \cup a$ e $X - a$ no lugar de $X \cup \{ a \}$ e $X - \{ a \}$, respectivamente.

[b] Vale a pena lembrar que o termo "matroide" é sinônimo do termo "matroide finita" neste texto.

[c] Quando não existir ambiguidade quanto à matroide M no contexto, vamos escrever E e $\mathcal{I}$ no lugar de $E(M)$ e $\mathcal{I}(M)$, respectivamente. Vamos usar também o termo "matroide sobre E" em algumas partes do texto para enfatizar o conjunto subjacente sobre o qual está definida a matroide.

são chamados de conjuntos *independentes* de M. Dizemos que duas matroides L e M são *isomorfas* e escrevemos $L \cong M$ quando existe uma bijeção $\varphi : E(L) \longrightarrow E(M)$ que satisfaz $\varphi[I] \in \mathcal{I}(M)$ sse $I \in \mathcal{I}(L)$.

EXEMPLO II.2.1 (Matroide Linear). [15, Proposição 1.1.1] O objetivo deste exemplo é mostrar como conjuntos independentes se manifestam em álgebra linear. Isso fornece uma espécie de guia moral que motiva ou ajuda no entendimento de certos resultados que serão obtidos sobre a independência abstrata. Suponhamos que A seja uma matriz de tamanho $m \times n$ com entradas em um corpo F e tomemos o conjunto E dos rótulos das colunas de A. Podemos identificar as colunas de A com vetores em $V(m, F)$[d]. Definamos a coleção $\mathcal{I}$ dos subconjuntos X de E para os quais o multiconjunto[e] das colunas de A rotuladas pelos elementos de X é linearmente independente. A coleção $\mathcal{I}$ é não-vazia e hereditária. Suponhamos que $I, J \in \mathcal{I}$ sejam tais $|I| < |J|$. Denotando por W o subespaço gerado pelas colunas rotuladas por $I \cup J$ em $V(m, F)$, vemos que $|J| \leq \dim W$. Se as colunas rotuladas por $I \cup a$ são linearmente dependentes para todo $a \in J - I$, então W está contido no subespaço gerado pelas colunas rotuladas por I. Isso permite escrever $|J| \leq \dim W \leq |I|$, o que contradiz $|I| < |J|$. Isto mostra que $\mathcal{I}$ tem a propriedade de aumento, e portanto, $(E, \mathcal{I})$ é uma matroide. Denotamos tal matroide por M(A) e dizemos que ela é uma *matroide linear.* ⊣

Dada uma matroide M, existem conjuntos independentes $\subseteq$-maximais em $\mathcal{I}(M)$ chamados de *bases* de M. A coleção das bases de uma matroide M é denotada por $\mathcal{B}(M)$. Observemos que $I \in \mathcal{I}(M)$ sse existe $B \in \mathcal{B}(M)$ tal que $I \subseteq B$. A Proposição II.2.2, que mostra que bases de matroides são equicardinais, é uma consequência imediata da definição de base e da propriedade de aumento dos conjuntos independentes de uma matroide.

PROPOSIÇÃO II.2.2. [15, Lema 1.2.1] Se $A, B \in \mathcal{B}(M)$, então $|A| = |B|$.

Bases de matroides possuem uma propriedade de troca semelhante à propriedade de troca de bases de espaços vetoriais[f]. Este resultado segue imediatamente da propriedade de aumento dos conjuntos independentes de uma matroide e da equicardinalidade de suas bases, como mostra a Proposição II.2.3.

PROPOSIÇÃO II.2.3. [15, Lema 1.2.2] Se $A, B \in \mathcal{B}(M)$ e $a \in A - B$, então existe $b \in B - A$ tal que $(A - a) \cup b \in \mathcal{B}(M)$.

Dada uma matroide M, dizemos que um subconjunto de E(M) que não é independente é *dependente.* Um *circuito* de M é um conjunto dependente $\subseteq$-minimal, i.e. $C \subseteq E(M)$ é um circuito sse C é dependente e $C - a$ é independente para todo $a \in C$. Circuitos unitários são chamados de *loops* e circuitos com apenas dois elementos são chamados de *pares paralelos*[g]. Denotamos por $\mathcal{C}(M)$ a coleção dos circuitos de M. Observemos que $\mathcal{C}(M)$ é uma anticadeia[h] e que $I \subseteq E(M)$ não contém circuitos sse $I \in \mathcal{I}(M)$. Isto se deve à minimalidade dos circuitos e à

[d] Vamos usar a notação adotada por J. Oxley [15] e denotar por $V(m, F)$ o espaço vetorial de dimensão m sobre o corpo F.

[e] Precisamos usar multiconjuntos para dar conta do caso das matrizes que possuem colunas iguais com rótulos distintos.

[f] A Proposição II.2.17 presente no final desta seção apresentará uma propriedade de troca ainda mais forte que bases de matroides também possuem.

[g] Usando o Exemplo II.2.1 como guia, vemos que em um espaço vetorial o vetor nulo é um loop e um par de vetores linearmente dependentes é um par paralelo.

[h] Em um conjunto parcialmente ordenado $(P, \leq)$, dizemos que dois elementos $p, q \in P$ são comparáveis quando vale $p \leq q$ ou $q \leq p$. Uma anticadeia em $(P, \leq)$ é um subconjunto $A \subseteq P$ de elementos dois a dois não-comparáveis quando distintos.

hereditariedade dos conjuntos independentes. Uma *classe paralela* é um conjunto $X \subseteq E(M)$ $\subseteq$-maximal tal que todo par de elementos distintos de X é um par paralelo e nenhum elemento de X é um loop[i]. Uma classe paralela é *trivial* sse é unitária. Dizemos que uma matroide é *simples* sse não possui loops ou classes paralelas não-triviais. Circuitos possuem uma propriedade de eliminação que é apresentada na Proposição II.2.4.

PROPOSIÇÃO II.2.4. [15, Lema 1.1.3] Se $C', C'' \in \mathcal{C}(M)$ são tais que $C' \neq C''$ e $a \in C' \cap C''$, então existe $C \in \mathcal{C}(M)$ tal que $C \subseteq (C' \cup C'') - a$.

Demonstração. Suponhamos que $(C' \cup C'') - a \in \mathcal{I}(M)$. Como $\mathcal{C}(M)$ é uma anticadeia, segue que existe $b \in C'' - C'$. Sabemos que $C'' - b \in \mathcal{I}(M)$. Tomemos $I \in \mathcal{I}(M)$ $\subseteq$-maximal dentre os conjuntos $J \in \mathcal{I}(M)$ tais que $C'' - b \subseteq J \subseteq C' \cup C''$. Existe $c \in C' - I$. Como $b \in C'' - C'$ e $C'' - b \subseteq I$, vemos que $c \neq b$. Temos $I - \{ b \cup c \} \subseteq (C' \cup C'') - \{ b \cup c \}$, e assim,

$$\begin{aligned} |I| &\leq |(C' \cup C'') - \{ b \cup c \}| \\ &= |C' \cup C''| - 2 \\ &< |(C' \cup C'') - a|. \end{aligned}$$

Segue da propriedade de aumento que existe $d \in (C' \cup C'') - a$ tal que $I \cup d \in \mathcal{I}(M)$. De $C'' - b \subseteq I \cup d \subseteq C' \cup C''$, obtemos uma contradição com a escolha de I. ⊣

A propriedade de eliminação dos circuitos é importante por caracterizar quais anticadeias são coleções de circuitos de matroides, como mostra o Teorema II.2.6. O seguinte lema será útil ao longo do texto e decorre da propriedade de eliminação.

LEMA II.2.5. [15, Proposição 1.1.6] Se $I \in \mathcal{I}(M)$ e $a \in E(M)$ são tais que $I \cup a \notin \mathcal{I}(M)$, então existe um único $C \in \mathcal{C}(M)$ tal que $a \in C$ e $C \subseteq I \cup a$.

Demonstração. Suponhamos que existam circuitos C' e C'' distintos e contidos em $I \cup a$. Como I é independente em M, segue que $a \in C' \cap C''$. Da Proposição II.2.4, existe um circuito C tal que $C \subseteq (C' \cup C'') - a \subseteq I$, o que contradiz a independência de I em M. ⊣

Dada uma base B de uma matroide M e $a \in E(M)$ tal que $a \notin B$, dizemos que o único circuito de M cuja existência é garantida pelo lema anterior é o *circuito fundamental de a com respeito à base* B e o denotamos por $C(a, B)$.

TEOREMA II.2.6 (Circuitos). [15, Teorema 1.1.4] Suponhamos que E seja um conjunto finito e que $\mathcal{C}$ seja uma anticadeia de subconjuntos de E que satisfaz a propriedade de eliminação da Proprosição II.2.4. A coleção $\mathcal{C}$ é a coleção dos circuitos de uma matroide sobre E cujos conjuntos independentes são aqueles que não contém elementos de $\mathcal{C}$.

Demonstração.

(1) A coleção $\mathcal{I}$ é não-vazia e hereditária. A parte restante da prova segue por redução ao absurdo. Suponhamos que existam $I, J \in \mathcal{I}$ com $|I| < |J|$ para os quais a propriedade de aumento falha. Sabemos que $I \neq \emptyset$. O conjunto $\{ X \subseteq I \cup J :$

[i] Usando o Exemplo II.2.1 como guia, vemos que uma classe paralela em um espaço vetorial é um conjunto finito de vetores não-nulos e colineares.

$|I| < |X|\}$ é não-vazio, uma vez que J pertence a este conjunto. Do Princípio da Boa Ordenação, segue que podemos tomar $I' \in \mathcal{I}$ tal que $I' \subseteq I \cup J$ e $|I| < |I'|$ minimizando $|I - I'|$. Observemos que vale $0 < |I - I'|$ pela escolha de $I, J \in \mathcal{I}$ e $I' \subseteq I \cup J$. Isto mostra que existe $a \in I - I'$.

(1.1) Vamos mostrar que dado $b \in I' - I$, existe $C_b \in \mathcal{C}$ tal que $a \in C_b$ e $b \notin C_b$. De fato, tomemos $I'_b = (I' - b) \cup a$. Observemos que $I'_b \subseteq I \cup J$ e $|I - I'_b| < |I - I'|$. Da escolha de $I' \in \mathcal{I}$, vemos que $I'_b \notin \mathcal{I}$. Existe $C_b \in \mathcal{C}$ tal que $C_b \subseteq I'_b$. De $I' - b \in \mathcal{I}$, obtemos $a \in C_b$.

(1.2) Vamos mostrar que $2 \leq |I' - I|$. De $|I| < |I'|$, sabemos que existe $x \in I' - I$. Consideremos C_x o circuito obtido do procedimento descrito no item 1.1 tomando $b = x$. Observemos que $C_x \cap (I' - I) \neq \emptyset$. De fato, se $C_x \cap (I' - I) = \emptyset$, então $C_x \subseteq (I' \cap I) \cup a \subseteq I$, o que é uma contradição. Isto mostra que existe $y \in C_x \cap (I' - I)$.

Segue dos dois itens anteriores que existem circuitos $C', C'' \in \mathcal{C}$ tais que $a \in C' \cap C''$ e $C' \neq C''$ com $C' \cup C'' \subseteq I' \cup a$. Da propriedade de eliminação, vemos que existe $C \in \mathcal{C}$ tal que $C \subseteq (C' \cup C'') - a \subseteq I'$, o que é uma contradição. Isto mostra que $M = (E, \mathcal{I})$ é uma matroide.

(2) Se $C' \subseteq E$ é um circuito de M, então dado $a \in C'$, temos $C' - a \in \mathcal{I}$. Disto segue que existe um único $C \in \mathcal{C}$ tal que $a \in C$ e $C \subseteq C'$. Por outro lado, sabemos que $C \notin \mathcal{I}$. Disto segue que existe um circuito C'' de M tal que $C'' \subseteq C$. Como circuitos formam anticadeias, segue que $C'' = C = C'$. Isto mostra que $\mathcal{C} = \mathcal{C}(M)$. ⊣

COROLÁRIO II.2.7. Suponhamos que L e M sejam matroides tais que $E(L) = E(M)$. Se todo circuito de L contém um circuito de M e todo circuito de M contém um circuito de L, então $L = M$.

EXEMPLO II.2.8 (Matroides Gráficas). [15, Proposição 1.1.7] O objetivo deste exemplo é mostrar como a dependência minimal se manifesta em grafos. Isso fornece uma espécie de guia moral e ajuda no entendimento de certos resultados que foram obtidos sobre circuitos de matroides. Suponhamos que G seja um grafo e que $\mathcal{C}(G)$ seja coleção dos circuitos de G. A coleção $\mathcal{C}(G)$ é uma anticadeia e satisfaz a propriedade de eliminação da Proposição II.2.4. De fato, suponhamos que $C_1, C_2 \in \mathcal{C}(G)$ sejam distintos e que exista uma aresta $e \in C_1 \cap C_2$.

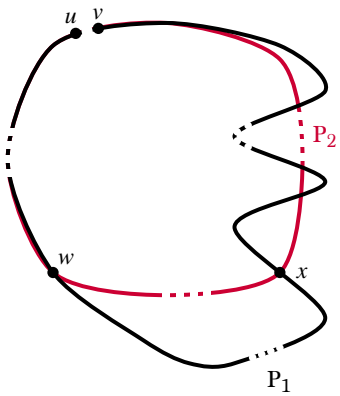

Figura II.2.1: Ilustração da propriedade de eliminação dos circuitos no caso concreto de matroides gráficas do Exemplo II.2.8.

Podemos supor que e incide a vértices u e v, como na Figura II.2.1. Denotemos por P_1 o (u,v)-caminho cujas arestas são $C_1 - e$ e por P_2 o (u,v)-caminho cujas arestas são $C_2 - e$. Partindo de u percorremos o caminho P_1 até o primeiro vértice w a partir do qual a próxima aresta de P_1 também não pertence ao caminho P_2. Continuamos percorrendo P_1 partindo de w até o vértice x (diferente de w) tal que x também pertença ao caminho P_2. Isso mostra que existe um ciclo de G que passa pelos vértices w e x e que evita e. O circuito obtido deste ciclo está contido em $(C_1 \cup C_2) - e$. Do Teorema II.2.6, é possível obter uma matroide $M(G) = (E(G), \mathcal{I}(G))$, na qual $\mathcal{I}(G)$ é a coleção dos conjuntos de arestas de florestas de G. Tal matroide é chamada de *matroide gráfica.* ⊣

Dados uma matroide M e um conjunto $X \subseteq E(M)$, podemos construir a matroide *restrição* $M \mid X$ pondo $E(M \mid X) = X$ e definindo $\mathcal{I}(M \mid X)$ como sendo a coleção dos conjuntos independentes de M contidos em X. Em virtude da Proposição II.2.2, podemos definir uma função $r_M : 2^{E(M)} \longrightarrow \mathbb{N}$ que associa cada conjunto $X \subseteq E(M)$ ao tamanho das bases da restrição $M \mid X$. Tal função é conhecida como *função posto* de M. Em particular, o *posto de* M é $r(M) = r_M(E(M))$.

PROPOSIÇÃO II.2.9. [15, Lema 1.3.1] Se M é uma matroide, então:

(1) Se $X \subseteq E(M)$, então $0 \leq r_M(X) \leq |X|$.

(2) Se $X, Y \subseteq E(M)$ e $X \subseteq Y$, então $r_M(X) \leq r_M(Y)$.

(3) Se $X, Y \subseteq E(M)$, então $r_M(X \cup Y) + r_M(X \cup Y) \leq r_M(X) + r_M(Y)$.

Demonstração. Vamos provar o terceiro item, uma vez que os itens anteriores têm demonstrações rotineiras. Suponhamos que A seja uma base de $M \mid X \cap Y$. Como A é independente em $M \mid X \cup Y$, segue que existe uma base B de $M \mid X \cup Y$ tal que $A \subseteq B$. Os conjuntos $B \cap X$ e $B \cap Y$ são independentes em $M \mid X$ e $M \mid Y$, respectivamente. Temos:

$$\begin{aligned} r_M(X \cup Y) + r_M(X \cap Y) &= |B| + |A| \\ &\leq |B \cap (X \cup Y)| + |B \cap (X \cap Y)| \\ &= |(B \cap X) \cup (B \cap Y)| + |(B \cap X) \cap (B \cap Y)| \\ &= |B \cap X| + |B \cap Y| \\ &\leq r_M(X) + r_M(Y). \end{aligned}$$ ⊣

A Proposição II.2.9 mostra que a função posto de uma matroide M é monótona e submodular em $2^{E(M)}$. Observemos que os elementos de $\mathcal{I}(M)$ são exatamente os elementos $I \subseteq E(M)$ tais que $r_M(I) = |I|$. Disto, vemos também que se $C \in \mathcal{C}(M)$, então $r_M(C) = |C| - 1$. Dados $X \subseteq E(M)$ e $a \in E(M)$, temos $r_M(X) \leq r_M(X \cup a) \leq r_M(X) + 1$.

EXEMPLO II.2.10 (Matroide Uniforme). [15, Exemplo 1.2.7] Vamos construir uma matroide especial chamada de matroide *uniforme* de posto r sobre um conjunto de m elementos, que denotaremos por $U_{r,m}$. Tal matroide é definida tomando um conjunto E de m elementos e impondo que $I \subseteq E$ seja independente sse $|I| \leq r$. Denotemos por $\mathcal{I}$ a coleção de tais conjuntos independentes. Dados $I, J \in \mathcal{I}$, suponhamos que $|I| < |J|$. Disto segue que existe $a \in J - I$. Temos $|I \cup a| = |I| + 1 \leq |J| \leq r$, e portanto, $I \cup a \in \mathcal{I}$. O par $U_{r,m} = (E, \mathcal{I})$ é de fato uma matroide. ⊣

LEMA II.2.11. [15, Lema 1.3.3] Suponhamos que E seja um conjunto finito e que $\varphi : 2^E \longrightarrow \mathbb{N}$ seja uma função que possui as propriedades apresentadas na Proposição II.2.9. Dados $X, Y \subseteq E$, se $\varphi(X \cup a) = \varphi(X)$ para todo $a \in Y - X$, então $\varphi(X \cup Y) = \varphi(X)$.

Demonstração. Dado $Z \subseteq Y - X$, se $|Z| = 1$, então temos $\varphi(X \cup Z) = \varphi(X)$ por hipótese. Suponhamos que o resultado seja válido para todo $S \subseteq Y - X$ com $|S| < m$ e tomemos $Z \subseteq Y - X$ com $|Z| = m$. Escrevamos $Z = R \cup S$, onde $|R| = m - 1$ e $|S| = 1$. Temos:

$$\begin{aligned}\varphi(X) + \varphi(X) &= \varphi(X \cup R) + \varphi(X \cup S) \\ &\geq \varphi((X \cup R) \cup (X \cup S)) + \varphi((X \cup R) \cap (X \cup S)) \\ &= \varphi(X \cup Z) + \varphi(X),\end{aligned}$$

e assim, $\varphi(X \cup Z) = \varphi(X)$. O resultado segue do Princípio de Indução. ⊣

O Teorema II.2.12 apresenta condições para que uma função seja a função posto de uma matroide. Este resultado será útil para obter alguns resultados sobre amálgamas próprias.

TEOREMA II.2.12 (Posto). [15, Teorema 1.3.2] Suponhamos que E seja um conjunto finito e que $\varphi : 2^E \longrightarrow \mathbb{N}$ seja uma função que possui as propriedades apresentadas na Proposição II.2.9. A função φ é a função posto de uma matroide sobre E cuja coleção de conjuntos independentes é $\mathcal{I} = \{ I \subseteq E : \varphi(I) = |I| \}$.

Demonstração.

(1) Definamos a coleção $\mathcal{I} = \{ I \subseteq E : \varphi(I) = |I| \}$. A coleção é não-vazia, uma vez que $\emptyset \in \mathcal{I}$. Mostremos primeiro que $\mathcal{I}$ é hereditária. Dados $I, J \subseteq E$, suponhamos que $J \in \mathcal{I}$ e $I \subseteq J$. Temos:

$$\begin{aligned}|J| &= \varphi(J) \\ &= \varphi(I \cup (J - I)) + \varphi(I \cap (J - I)) \\ &\leq \varphi(I) + \varphi(J - I) \\ &\leq |I| + |J - I| \\ &= |I \cap J| + |J - I| \\ &= |J|.\end{aligned}$$

Assim, $\varphi(I) = |I|$, e portanto, $I \in \mathcal{I}$. Mostremos agora que $\mathcal{I}$ possui a propriedade de aumento. Suponhamos que existam $I, J \in \mathcal{I}$ com $|I| < |J|$ de modo que para todo $a \in J - I$ tenhamos $I \cup a \notin \mathcal{I}$. Disto vemos que

$$\begin{aligned}\varphi(I \cup a) &< |I \cup a| \\ &= |I| + 1 \\ &= \varphi(I) + 1,\end{aligned}$$

e portanto, $\varphi(I \cup a) \leq \varphi(I)$. Disto e de $\varphi(I) \leq \varphi(I \cup a)$, obtemos $\varphi(I \cup a) = \varphi(I)$. Do Lema II.2.11, obtemos $\varphi(I \cup J) = \varphi(I)$. Por outro lado, sabemos que $\varphi(J) \leq \varphi(I \cup J)$. De $I, J \in \mathcal{I}$, segue que $|J| \leq |I|$, o que é uma contradição. Isto mostra que $M = (E, \mathcal{I})$ é uma matroide.

(2) Para todo $I \in \mathcal{I}$ vale $\varphi(I) = r_M(I)$. Dado $X \notin \mathcal{I}$, tomemos B uma base de $M \mid X$. Temos $r_M(X) = |B|$. Dado $a \in X - B$, temos $B \cup a \notin \mathcal{I}$. Segue então que $|B| = \varphi(B) \leq \varphi(B \cup a) < |B \cup a|$, e assim, $\varphi(B \cup a) = \varphi(B)$. Do Lema II.2.11, temos $\varphi(X \cup B) = \varphi(B)$. Como $B \subseteq X$, segue que $\varphi(X) = r_M(X)$. Isso mostra que φ é a função posto da matroide M. ⊣

Podemos construir uma função $\mathrm{cl_M} : 2^{\mathrm{E(M)}} \longrightarrow 2^{\mathrm{E(M)}}$ que associa cada conjunto $\mathrm{X} \subseteq \mathrm{E(M)}$ à união disjunta

$$\mathrm{cl_M(X)} = \mathrm{X} \cup \partial_{\mathrm{M}}(\mathrm{X}),$$

onde $\partial_{\mathrm{M}}(\mathrm{X}) = \{\, a \in \mathrm{E(M)} - \mathrm{X} : \exists \mathrm{C} \in \mathcal{C}(\mathrm{M}) \;\; a \in \mathrm{C} \text{ e } \mathrm{C} \subseteq \mathrm{X} \cup a \,\}$[j]. Tal função é conhecida como *operador de fecho* de M. Observemos que se $a \in \mathrm{E(M)}$ e $\mathrm{I} \in \mathcal{I}(\mathrm{M})$ são tais que $\mathrm{I} \cup a \notin \mathcal{I}(\mathrm{M})$, então $a \in \mathrm{cl_M(I)}$. O segundo item da Proposição II.2.13 mostra que o operador de fecho é idempotente. Já o primeiro item da mesma proposição mostra que o fecho de um conjunto é o maior conjunto de mesmo posto que o contém.

PROPOSIÇÃO II.2.13. Se M é uma matroide, então:

(1) Dados $a \in \mathrm{E(M)}$ e $\mathrm{X} \subseteq \mathrm{E(M)}$, temos $a \in \mathrm{cl_M(X)}$ sse $r_{\mathrm{M}}(\mathrm{X} \cup a) = r_{\mathrm{M}}(\mathrm{X})$. Mais ainda, vale $r_{\mathrm{M}}(\mathrm{X}) = r_{\mathrm{M}}(\mathrm{cl_M(X)})$.

(2) [15, Item **CL3** do Lema 1.4.2] Dado $\mathrm{X} \subseteq \mathrm{E(M)}$, temos $\mathrm{cl_M(cl_M(X))} = \mathrm{cl_M(X)}$.

Demonstração.

(1) Dados $a \in \mathrm{E(M)}$ e $\mathrm{X} \subseteq \mathrm{E(M)}$, suponhamos que $r_{\mathrm{M}}(\mathrm{X} \cup a) = r_{\mathrm{M}}(\mathrm{X})$. Dada uma base B de $\mathrm{M} \mid \mathrm{X} \cup a$, vemos que B é uma base de $\mathrm{M} \mid \mathrm{X}$. Existe um único $\mathrm{C} \in \mathcal{C}(\mathrm{M})$ tal que $a \in \mathrm{C}$ e $\mathrm{C} \subseteq \mathrm{B} \cup a$. Como $\mathrm{B} \subseteq \mathrm{X}$, obtemos $a \in \mathrm{cl_M(X)}$. Por outro lado, dados $a \in \mathrm{E(M)}$ e $\mathrm{X} \subseteq \mathrm{E(M)}$, suponhamos que $a \in \mathrm{cl_M(X)}$. Podemos supor que $a \in \partial_{\mathrm{M}}(\mathrm{X})$. Nesse caso, vemos que $\mathrm{X} \cup a \notin \mathcal{I}(\mathrm{M})$, e assim, $r_{\mathrm{M}}(\mathrm{X} \cup a) = r_{\mathrm{M}}(\mathrm{X})$. Mais ainda, do Lema II.2.11, temos $r_{\mathrm{M}}(\mathrm{X}) = r_{\mathrm{M}}(\mathrm{cl_M(X)})$.

(2) Dado $a \in \mathrm{cl_M(cl_M(X))}$, segue do primeiro item que $r_{\mathrm{M}}(\mathrm{cl_M(X)} \cup a) = r_{\mathrm{M}}(\mathrm{cl_M(X)})$. Para todo $b \in \partial_{\mathrm{M}}(\mathrm{X})$, segue também do primeiro item que $r_{\mathrm{M}}(\mathrm{X} \cup b) = r_{\mathrm{M}}(\mathrm{X})$. Do Lema II.2.11, temos $r_{\mathrm{M}}(\mathrm{X}) = r_{\mathrm{M}}(\mathrm{cl_M(X)})$. Disto tudo, obtemos $r_{\mathrm{M}}(\mathrm{X}) = r_{\mathrm{M}}(\mathrm{cl_M(X)} \cup a)$, e portanto,

$$\begin{aligned} r_{\mathrm{M}}(\mathrm{X}) &= r_{\mathrm{M}}(\mathrm{cl_M(X)} \cup a) \\ &\geq r_{\mathrm{M}}(\mathrm{X} \cup a) \\ &\geq r_{\mathrm{M}}(\mathrm{X}). \end{aligned}$$

Concluímos que $a \in \mathrm{cl_M(X)}$. ⊣

Os conjuntos $\mathrm{F} \subseteq \mathrm{E(M)}$ que satisfazem $\mathrm{cl_M(F)} = \mathrm{F}$ são chamados de *flats* de M. Em virtude da Proposição II.2.13, vemos que $\mathrm{cl_M(X)}$ é um flat de M, qualquer que seja $\mathrm{X} \subseteq \mathrm{E(M)}$. As seguintes propriedades do operador de fecho são fundamentais:

PROPOSIÇÃO II.2.14. [15, Lema 1.4.2] Se M é uma matroide, então:

(1) Dados $\mathrm{X}, \mathrm{Y} \subseteq \mathrm{E(M)}$, vale $\mathrm{X} \subseteq \mathrm{cl_M(Y)}$ sse $\mathrm{cl_M(X)} \subseteq \mathrm{cl_M(Y)}$.

(2) Dados $\mathrm{X} \subseteq \mathrm{E(M)}$ e $a, b \in \mathrm{E(M)}$, se $a \in \mathrm{cl_M(X} \cup b) - \mathrm{cl_M(X)}$, então $b \in \mathrm{cl_M(X} \cup a)$. Esta propriedade é conhecida como *propriedade de troca de Steinitz-Mac Lane.*

[j] Podemos interpretar este conjunto no caso concreto de uma matroide gráfica (vide Exemplo II.2.8) de maneira bem natural. Suponhamos que G seja um grafo, que $\mathrm{M} = \mathrm{M(G)}$ seja a matroide gráfica obtida deste grafo e que $\mathrm{X} \subseteq \mathrm{E(M)}$. O conjunto $\partial_{\mathrm{M}}(\mathrm{X})$ é formado pelas arestas de $\mathrm{G} \mid \mathrm{E(M)} - \mathrm{X}$ que induzem circuitos em $\mathrm{G} \mid \mathrm{X}$ ao serem adicionadas a este grafo.

Demonstração.

(1) Dados X, Y $\subseteq$ E(M), suponhamos que X $\subseteq$ $\mathrm{cl_M}$(Y). Se $a \in \partial_{\mathrm{M}}(\mathrm{X})$, então existe C $\in \mathcal{C}$(M) tal que $a \in$ C e C $\subseteq$ X $\cup\, a$. Disto segue que C $\subseteq$ $\mathrm{cl_M}$(Y) $\cup\, a$. Do segundo item da Proposição II.2.13, temos $a \in \mathrm{cl_M}(\mathrm{cl_M}(\mathrm{Y})) = \mathrm{cl_M}(\mathrm{Y})$, e portanto, $\mathrm{cl_M}(\mathrm{X}) \subseteq \mathrm{cl_M}(\mathrm{Y})$. A outra condicional é direta.

(2) Podemos supor que $a \neq b$ e que $a \in \mathrm{cl_M}(\mathrm{X} \cup b) - \mathrm{cl_M}(\mathrm{X})$. Vamos mostrar que $b \in \mathrm{cl_M}(\mathrm{X} \cup a)$. Existe C $\in \mathcal{C}$(M) tal que $a \in$ C e C $\subseteq$ X $\cup$ ($b \cup a$). Devemos ter $b \in$ C. De fato, se $b \notin$ C, então C = C $- b \subseteq$ X $\cup\, a$, e assim, $a \in \mathrm{cl_M}(\mathrm{X})$, o que é uma contradição. Por redução ao absurdo, segue que $a, b \in$ C, e portanto, $b \in \mathrm{cl_M}(\mathrm{X} \cup a)$. ⊣

O primeiro item da Proposição II.2.14 justifica o nome "fecho" para o operador. A propriedade de troca de Steinitz-Mac Lane caracteriza operadores de fecho que são fechos matroidais, como mostra o Teorema II.2.15. Este resultado será útil para obter alguns resultados sobre amálgamas próprias.

TEOREMA II.2.15 (Fecho). [15, Teorema 1.4.4] Suponhamos que E seja um conjunto finito e que $\varphi : 2^{\mathrm{E}} \longrightarrow 2^{\mathrm{E}}$ seja um operador de fecho que satisfaz a propriedade de troca de Steinitz-Mac Lane da Proposição II.2.14. A função φ é o operador de fecho de uma matroide sobre E cuja coleção dos conjuntos independentes é $\mathcal{I} = \{\, \mathrm{I} \in 2^{\mathrm{E}} : \neg\exists a \in \mathrm{I}\ a \in \varphi(\mathrm{I} - a) \,\}$.

Antes de iniciarmos a demonstração do Teorema II.2.15, façamos uma pequena discussão sobre o significado deste resultado em um caso concreto. No contexto de Álgebra Linear, interpretamos o fecho de um conjunto X de vetores como subespaço gerado pelos vetores de X. Todo elemento deste subespaço é uma combinação linear dos elementos de X. Um conjunto X é linearmente independente quando a única combinação linear possível dos vetores de X que resulta no vetor nulo é aquela em que todos os coeficientes são nulos. Isso quer dizer que um vetor x de um conjunto linearmente independente X não pode pertencer ao fecho do conjunto X $- x$. Essa discussão motiva e torna mais natural o resultado do teorema que devemos provar. Antes de seguir para a demostração do teorema, provemos a seguinte afirmação:

Afirmação 1. [15, Lema 1.4.5] Suponhamos que $\varphi : 2^{\mathrm{E}} \longrightarrow 2^{\mathrm{E}}$ seja um operador de fecho que satisfaz a propriedade de troca de Steinitz-Mac Lane da Proposição II.2.14. Se I $\in \mathcal{I}$ e $a \in$ E $-$ I são tais que I $\cup\, a \notin \mathcal{I}$, então $a \in \varphi$(I).

Demonstração. Como I $\cup\, a \notin \mathcal{I}$, segue que existe $b \in$ I $\cup\, a$ tal que $b \in \varphi((\mathrm{I} \cup a) - b)$. Podemos supor que $b \neq a$ e escrever (I $\cup\, a$) $- b$ = (I $- b$) $\cup\, a$. De $b \in$ I e I $\in \mathcal{I}$, obtemos $b \notin \varphi(\mathrm{I} - b)$. Disto, vemos que $b \in \varphi((\mathrm{I} - b) \cup a) - \varphi(\mathrm{I} - b)$. Da propriedade de troca de Steinitz-Mac Lane, obtemos $a \in \varphi((\mathrm{I} - b) \cup b) = \varphi(\mathrm{I})$. ⊣

Passemos agora para a demonstração do Teorema II.2.15:

Demonstração.

(1) A coleção $\mathcal{I}$ é não-vazia e hereditária. Suponhamos que existam I, J $\in \mathcal{I}$ tais que para todo $a \in$ J $-$ I, tenhamos I $\cup\, a \notin \mathcal{I}$. Podemos supor que I e J são tais que $|\mathrm{I} \cap \mathrm{J}|$ é maximal. Tomemos $a \in$ J $-$ I. Vale I $\nsubseteq \varphi$(J $- a$). De fato, se I $\subseteq \varphi$(J $- a$), então φ(I) $\subseteq \varphi$(J $- a$). Como J $\in \mathcal{I}$, vemos que $a \notin \varphi$(J $- a$), e assim, $a \notin \varphi$(I).

Disto e da Afirmação 1, segue que $I \cup a \in \mathcal{I}$, o que é uma contradição. Isto mostra que existe $b \in I - \varphi(J - a)$, e portanto, $b \in I - J$. Tomemos $J' = (J - a) \cup b$. Como $a \in J - I$ e $b \in I - J$, vemos que $|I \cap J| < |I \cap J'|$. Existe $c \in J' - I$ tal que $I \cup c \in \mathcal{I}$. Por outro lado, $c \in J' - I$ implica em $c \in J - a$ e $c \notin I$. Disto, vemos que $c \in J - I$ com $c \neq a$ é tal que $I \cup c \in \mathcal{I}$, o que é uma contradição. Isto mostra que $M = (E, \mathcal{I})$ é uma matroide.

(2) Tomemos $X \subseteq E$ qualquer. Para cada $a \in \partial_M(X)$, segue da Proposição II.2.13 que $r_M(X \cup a) = r_M(X)$. Suponhamos que B seja uma base de $M \mid X$. Temos $B \cup a \notin \mathcal{I}$. Da Afirmação 1, segue $a \in \varphi(B) \subseteq \varphi(X)$. Disto, vemos que $\mathrm{cl}_M(X) \subseteq \varphi(X)$. Por outro lado, tomemos $a \in \varphi(X) - X$. Suponhamos que B seja uma base de $M \mid X$. Temos $X \subseteq \varphi(B)$, e portanto, $\varphi(X) \subseteq \varphi(B)$. Disto, segue que $B \cup a \notin \mathcal{I}$ para cada $a \in X - B$, e assim, B é uma base de $M \mid X \cup a$. Temos $r_M(X \cup a) = |B| = r_M(X)$ e da Proposição II.2.13, segue $a \in \mathrm{cl}_M(X)$. Disto, segue que $\varphi(X) \subseteq \mathrm{cl}_M(X)$. Isto mostra que φ é o operador de fecho da matroide M. ⊣

A seguinte Proposição II.2.16 é consequência direta da Proposição II.2.14. Basta lembrar que se M é uma matroide e $X \subseteq E(M)$, então $\mathrm{cl}_M(X)$ é o maior subconjunto de E(M) que contém X e que satisfaz $r_M(\mathrm{cl}_M(X)) = r_M(X)$. O resultado será utilizado em um passo da demonstração do Lema III.5.2.

PROPOSIÇÃO II.2.16. [15, Exercício 1(iii) sec. 1.4] Dados $X, Y \subseteq E(M)$, se $X \subseteq Y$ e $r_M(X) = r_M(Y)$, então $\mathrm{cl}_M(X) = \mathrm{cl}_M(Y)$.

Os teoremas desta seção mostram que podemos especificar uma mesma matroide por seus conjuntos independentes, seus circuitos, sua função posto ou seu operador de fecho. Podemos formar pares $(E, \mathcal{C})$, (E, r) e (E, cl). Se $(E, \mathcal{I})$ é uma matroide e $\mathcal{C}$, r e cl são a coleção dos circuitos, a função posto e o operador de fecho de $(E, \mathcal{I})$, respectivamente, então dizemos que $(E, \mathcal{C})$, (E, r) e (E, cl) são *criptomorfas* à matroide $(E, \mathcal{I})$. Esta noção de criptomorfismo será útil para entender os resultados da Seção III.6. A Teoria de Matroides admite um princípio de dualidade e a noção de matroide dual será importante para descrever o conceito de menores de uma matroide [15]. Antes de explicitar a matroide dual, precisamos estabelecer certos resultados preliminares sobre candidatos a bases da matroide dual.

PROPOSIÇÃO II.2.17. Se $A, B \in \mathcal{B}(M)$ e $a \in A - B$, então existe $x \in B - A$ tal que $(A - a) \cup x \in \mathcal{B}(M)$ e $(B - x) \cup a \in \mathcal{B}(M)$.

Demonstração. Suponhamos que existam bases A e B de M e $a \in A - B$ falseando a afirmação do enunciado. Podemos supor que A e B são tais que $|A \triangle B|$ é minimal. Em virtude da Proposição II.2.3, existe $x \in B - A$ tal que $A_1 = (A - a) \cup x$ é uma base de M. Da suposição inicial, segue que $B_1 = (B - x) \cup a$ não é uma base de M. Mais ainda, vemos que B_1 é um conjunto dependente de M. Por outro lado, da existência de $x \in B - A$ e da Proposição II.2.3, segue que existe $b \in A - B$ tal que $B_2 = (B - x) \cup b$ é uma base de M. Observemos que $|A \triangle B_2| < |A \triangle B|$, e portanto, segue da escolha de A e B que existe $y \in B_2 - A$ tal que $A_2 = (A - a) \cup y$ e $B_3 = (B_2 - y) \cup a$ são bases de M. Como $A_2 = (A - a) \cup y$ é uma base de M e o enunciado não vale para A e B, vemos que $B_4 = (B - y) \cup a$ é dependente em M. Com isso, obtemos os conjuntos dependentes B_1 e B_4. Existem únicos circuitos distintos C_1 e C_4 tais que $a \in C_1 \cap C_4$ e que satisfazem $C_1 \subseteq B_1$ e $C_4 \subseteq B_4$. Disto, segue que existe um circuito C tal que $C \subseteq (C_1 \cup C_4) - a$. Podemos escrever $B_3 = [B - (x \cup y)] \cup (a \cup b)$, e portanto, $C \subseteq B_3$, o que é uma contradição. ⊣

Denotemos por $\mathcal{B}^*(M)$ a coleção dos complementares das bases de uma matroide M. Os elementos de $\mathcal{B}^*(M)$ são chamados de *cobases* da matroide M. Segue da Proposição II.2.17 que se $A^*, B^* \in \mathcal{B}^*(M)$ e $a \in A^* - B^*$, então existe $x \in B^* - A^*$ tal que $(A^* - a) \cup x \in \mathcal{B}^*(M)$. O seguinte lema segue da equicardinalidade das bases de uma matroide.

LEMA II.2.18. Dados $A^*, B^* \in \mathcal{B}^*(M)$, vale $|A^*| = |B^*|$.

A *matroide dual* M^* de uma matroide M é a matroide cuja coleção de bases é a coleção das cobases de M. Em virtude do *princípio da dualidade*, vemos que teoremas sobre matroides duais são teoremas sobre matroides. Observemos que a dualização é uma involução, i.e. $M^{**} = M$. Os conjuntos independentes da matroide dual M^* são chamados de conjuntos *coindependentes* da matroide M. Dizemos que $S \subseteq E(M)$ é um conjunto *gerador* de M quando $\mathrm{cl}_M(S) = E(M)$. Observemos que as bases de M são conjuntos geradores minimais de M. Segue desta observação que complementares de conjuntos coindependentes de M são conjuntos geradores de M[k].

PROPOSIÇÃO II.2.19. [15, Lema 2.1.10] Suponhamos que $I \in \mathcal{I}(M)$ e $I^* \in \mathcal{I}(M^*)$ sejam disjuntos. Existem $B \in \mathcal{B}(M)$ e $B^* \in \mathcal{B}(M^*)$ disjuntas tais que $I \subseteq B$ e $I^* \subseteq B^*$.

Demonstração. O conjunto I é independente em $M \mid E(M) - I^*$. Tomemos $B \subseteq E(M)$ uma base de $M \mid E(M) - I^*$. Neste caso, vemos que $r_M(B) = r_M(E(M) - I^*) = r(M)$, e portanto, $B \in \mathcal{B}(M)$. Tomando $B^* = E(M) - B$, obtemos $I \subseteq B$ e $I^* \subseteq B^*$. ⊣

Um problema importante é caracterizar a função posto de M^* partindo da função posto de M. Isto é feito na Proposição II.2.20, que será importante para obter certos resultados sobre certos tipos de matroides especiais.

PROPOSIÇÃO II.2.20. [15, Proposição 2.1.9] A função posto de M^* é $r_{M^*}(X) = |X| + r_M(E(M) - X) - r(M)$.

Demonstração. Dado $X \subseteq E(M)$, tomemos uma base B^* de $M^* \mid X$ e uma base B de $M \mid E(M) - X$. Da Proposição II.2.19, existem $A \in \mathcal{B}(M)$ e $A^* \in \mathcal{B}(M^*)$ disjuntas tais que $B \subseteq A$ e $B^* \subseteq A^*$. Temos $A^* = E(M) - A$, e assim, $X = (X \cap A) \cup (X \cap A^*)$ é uma união disjunta. Observemos que $A \cap (E(M) - X) = B$ e $A^* \cap X = B^*$. Temos $A = [A \cap (E(M) - X)] \cup (A \cap X)$, e portanto:

$$\begin{aligned} r(M) &= |A| \\ &= |B| + |A \cap X| \\ &= |B| + |X| - |X \cap A^*| \\ &= |B| + |X| - |B^*| \\ &= r_M(E(M) - X) + |X| - r_{M^*}(X). \end{aligned}$$

Disto, concluímos que $r_{M^*}(X) = |X| + r_M(E(M) - X) - r(M)$. ⊣

[k] Esta sentença parece confusa, mas não é quando a analisamos mais de perto. Suponhamos que I^* seja um conjunto coindependente de $M = (E, \mathcal{I})$. Neste caso, vemos que existe uma cobase B^* de M tal que $I^* \subseteq B^*$. Existe uma base B de M tal que $B^* = E - B$, e assim, $B \subseteq E - I^*$. Como bases de M são conjuntos geradores (minimais) de M, vemos que $E = \mathrm{cl}_M(B) \subseteq \mathrm{cl}_M(E - I^*)$. Isto mostra que $r_M(E - I^*) = r(M)$.

II.3 MATROIDES LINEARMENTE REPRESENTÁVEIS

Apresentaremos nesta seção o conceito de representabilidade linear de matroides e menores de uma matroide. A referência principal desta seção é J. Oxley [15]. Suponhamos que p seja um número inteiro primo positivo, que m seja um número natural positivo e tomemos $q = p^m$. Denotemos por $\mathrm{GF}(q)$ o corpo com q elementos[1]. Caso $\mathrm{F} = \mathrm{GF}(q)$, escreveremos $\mathrm{V}(r, q)$ no lugar de $\mathrm{V}(r, \mathrm{GF}(q))$.

Dizemos que uma matroide simples M é *linearmente* F-*representável* quando existe uma uma função $\varphi : \mathrm{E(M)} \longrightarrow \mathrm{V}(r(\mathrm{M}), \mathrm{F})$ tal que para todo $\mathrm{X} \subseteq \mathrm{E(M)}$ vale $\mathrm{X} \in \mathcal{I}(\mathrm{M})$ sse $|\varphi[\mathrm{X}]| = |\mathrm{X}|$ e $\varphi[\mathrm{X}]$ é linearmente independente em $\mathrm{V}(r(\mathrm{M}), \mathrm{F})$. Fazendo $m = |\mathrm{E(M)}|$, podemos enumerar os elementos de E(M) na forma e_1, ..., e_m e construir uma matriz $\mathrm{A} = [\ \varphi(e_1) \cdots \varphi(e_m)\ ]$. Isso mostra que $\mathrm{M} \cong \mathrm{M(A)}$, onde M(A) é a matroide obtida analisando a independência linear das m colunas de A seguindo o que foi feito no Exemplo II.2.1. Nesse caso dizemos que A é uma matriz representante de M. A matroide M é *linearmente representável* quando existe um corpo F tal que M é linearmente F-representável. A matroide M(A) não determina a matriz A unicamente, uma vez que operações elementares sobre as linhas de A preservam a independência de suas colunas. Isto quer dizer que M(A) não é alterada quando aplicamos operações elementares sobre as linhas de A [15].

LEMA II.3.1. [15, Teorema 2.2.8] Suponhamos que M seja uma matroide com n elementos e posto r tal que $0 < r < n$. Se $\mathrm{M} \cong \mathrm{M(A)}$, onde $\mathrm{A} = [\ \mathrm{I}_r\ \mathrm{D}\ ]$, então $\mathrm{M}^* \cong \mathrm{M}(\mathrm{A}^*)$, onde $\mathrm{A}^* = [\ -\mathrm{D}^\top\ \mathrm{I}_{n-r}\ ]$.

Demonstração. Escrevamos $\mathrm{E} = \mathrm{E(M)}$. Tomemos $\mathrm{B} \in \mathcal{B}(\mathrm{M})$. Ao rearranjarmos as colunas e linhas de A, rearranjamos as linhas e colunas de A^*. Uma vez que operações elementares sobre linhas não alteram a independência das colunas, podemos supor que $\mathrm{B} = \{\, b_{r-t+1}, \ldots, b_r, b_{r+1}, \ldots, b_{2r-t}\,\}$ para algum $t \in [0, r]$. Podemos particionar A em blocos da forma:

$$\begin{bmatrix} \mathrm{I}_{r-t} & 0 & \mathrm{D}_1 & \mathrm{D}_2 \\ 0 & \mathrm{I}_t & \mathrm{D}_3 & \mathrm{D}_4 \end{bmatrix}.$$

O bloco formado por 0, D_1, I_t e D_3 corresponde à base B, e o posto de tal submatriz é r. Isso mostra que D_1 e $-\mathrm{D}_1^\top$ têm posto $r - t$. A partição em blocos feita em A induz a seguinte partição em blocos em A^*:

$$\begin{bmatrix} -\mathrm{D}_1^\top & -\mathrm{D}_3^\top & \mathrm{I}_{r-t} & 0 \\ -\mathrm{D}_2^\top & -\mathrm{D}_4^\top & 0 & \mathrm{I}_{n-(2r-t)} \end{bmatrix}.$$

A submatriz correspondente a $\mathrm{E} - \mathrm{B}$ em A^* é formada pelos blocos $-\mathrm{D}_1^\top$, 0, $-\mathrm{D}_2^\top$ e $\mathrm{I}_{n-(2r-t)}$. O posto desta submatriz é $(r-t) + (n-(2r-t)) = n - r$. Isto mostra que $\mathrm{E} - \mathrm{B} \in \mathcal{B}(\mathrm{M}^*)$. Dado $\mathrm{B}^* \in \mathcal{B}(\mathrm{M}^*)$, podemos usar o mesmo tipo de argumento para mostrar que $\mathrm{E} - \mathrm{B}^* \in \mathcal{B}(\mathrm{M})$. Concluímos que $\mathrm{M}^* \cong \mathrm{M}(\mathrm{A}^*)$. ⊣

TEOREMA II.3.2 (Representabilidade da Matroide Dual). [15, Corolário 2.2.9] Se M é uma matroide linearmente F-representável, então M^* é uma matroide linearmente F-representável.

[1] Assim como foi feito na seção anterior para espaços vetoriais, vamos usar a notação adotada por J. Oxley [15] para corpos finitos.

Demonstração. Escrevamos $n = |E(M)|$. Se M e M^* têm posto positivo menor que n, então o resultado segue do Lema II.3.1. Se o posto de M é zero, então $M \cong U(0, n)$, e assim, $M^* = U(n, n)$ (Vide Exemplo II.2.10). Se o posto de M é n, então $M \cong U(n, n)$, e assim, $M^* = U(0, n)$ (Vide Exemplo II.2.10). Em todo caso vale o resultado. ⊣

Um *coloop* de uma matroide M é um elemento que pertence à interseção de todas as bases de M, ou equivalentemente, é um loop da matroide dual M^*. Podemos construir novas matroides partindo de uma matroide simples M por remoções de seus elementos. Suponhamos que M seja uma matroide simples e que $a \in E(M)$. A *deleção* de a em M é a matroide $M \setminus a = M \mid E(M) - a$. A *contração* de a em M é a matroide $M / a = (M^* \setminus a)^*$. Segue do Teorema II.3.2 que se M é linearmente F-representável, então $M \setminus a$ e M / a são linearmente F-representáveis. Dado $X \subseteq E(M)$, definamos a deleção $M \setminus X = M \mid E(M) - X$ e a contração $M / X = (M^* \setminus X)^*$. Observemos que $E(M \setminus X) = E(M / X)$. A Proposição II.3.3 a seguir apresenta caracterizações das funções posto de contrações e deleções com respeito à função posto da matroide original.

PROPOSIÇÃO II.3.3. Suponhamos que M seja uma matroide e que $X \subseteq E(M)$. Temos:

(1) [15, Resultado 3.1.5] Para todo $Y \subseteq E(M \setminus X)$ vale $r_{M\setminus X}(Y) = r_M(Y)$.

(2) [15, Proposição 3.1.6] Para todo $Y \subseteq E(M / X)$ vale $r_{M/X}(Y) = r_M(X \cup Y) - r_M(X)$.

Demonstração.

(1) Dado $Y \subseteq E(M) - X$ sabemos que $r_M(Y)$ é o cardinal de uma base da restrição $M \mid Y$, e portanto, $r_{M\setminus X}(Y) = r_M(Y)$.

(2) Para todo $Y \subseteq E(M) - X$ vale $r_{M/X}(Y) = r_{(M^*\setminus X)^*}(Y)$. Sabemos que $E(M) - (X \cap Y) = (E(M) - X) \cup (E(M) - Y)$ e $E(M) - (X \cup Y) = (E(M) - X) \cap (E(M) - Y)$. De $Y \subseteq E(M) - X$, obtemos $X \cap Y = \emptyset$, e portanto,

$$|E(M)| + |E(M) - (X \cup Y)| = |E(M) - X| + |E(M) - Y|.$$

Disto, segue que $|Y| + |E(M) - (X \cup Y)| - |E(M) - X| = 0$. Da Proposição II.2.20 e do item anterior, segue que:

$$\begin{aligned} r_{M/X}(Y) &= |Y| + r_{M^*\setminus X}(E(M) - (X \cup Y)) - r_{M^*\setminus X}(E(M) - X) \\ &= |Y| + r_{M^*}(E(M) - (X \cup Y)) - r_{M^*}(E(M) - X) \\ &= |Y| + |E(M) - (X \cup Y)| + r_M(X \cup Y) - r_M(E(M)) + \\ &\quad r_M(E(M)) - |E(M) - X| - r_M(X) \\ &= |Y| + |E(M) - (X \cup Y)| - |E(M) - X| + r_M(X \cup Y) - r_M(X) \\ &= r_M(X \cup Y) - r_M(X). \end{aligned}$$ ⊣

Da Proposição II.3.3, segue que se $a \in E(M)$ é um loop ou coloop, então $M / a = M \setminus a$. A Proposição II.3.4 a seguir será útil para definir menores de uma matroide. Os resultados da proposição permitirão escrever sequências finitas de contrações e deleções de certa maneira especial.

PROPOSIÇÃO II.3.4. [15, Proposição 3.1.26] Suponhamos que M seja uma matroide e que $X, Y \subseteq E(M)$ sejam disjuntos. Valem:

(1) $(M \setminus X) \setminus Y = M \setminus (X \cup Y)$.

(2) $(M / X) / Y = M / (X \cup Y)$.

(3) $(M \setminus X) / Y = (M / Y) \setminus X$.

Demonstração.

(1) Observemos que $(M\setminus X)\setminus Y = M \mid E(M\setminus X) - Y$. Disto e de $E(M\setminus X) = E(M) - X$, obtemos $(M \setminus X) \setminus Y = M \setminus (X \cup Y)$.

(2) Da definição de contração e do item anterior, obtemos:

$$\begin{aligned}(M / X) / Y &= ((M / X)^* \setminus Y)^* \\ &= ((M^* \setminus X)^{**} \setminus Y)^* \\ &= ((M^* \setminus X) \setminus Y)^* \\ &= (M^* \setminus (X \cup Y))^* \\ &= M / (X \cup Y).\end{aligned}$$

(3) Dado $Z \subseteq E(M) - (X \cup Y)$, segue da Proposição II.3.3 que

$$\begin{aligned}r_{(M\setminus X)/Y}(Z) &= r_{M\setminus X}(Y \cup Z) - r_{M\setminus X}(Y) \\ &= r_M(Y \cup Z) - r_M(Y) \\ &= r_{M/Y}(Z) \\ &= r_{(M/Y)\setminus X}(Z).\end{aligned}$$

Isso mostra que $\mathcal{I}((M\setminus X)/Y) = \mathcal{I}((M/Y)\setminus X)$, e assim, $(M\setminus X)/Y = (M/Y)\setminus X$. ⊣

Suponhamos que M seja uma matroide e que $X, Y \subseteq E(M)$ sejam conjuntos disjuntos. A matroide $M \setminus X / Y$ é chamada de *menor* da matroide M. Quando $X \cup Y \neq \emptyset$, dizemos que o menor $M \setminus X / Y$ é próprio. Dadas três matroides L, M e N, dizemos que L é um M-menor de N quando L é um menor de N isomorfo à M. Quando existe um M-menor de N, escrevemos $M \preceq N$. Do Teorema II.3.2, obtemos o seguinte resultado:

TEOREMA II.3.5 (Menores Representáveis). [15, Proposição 3.2.4] Suponhamos que M e N sejam matroides. Se M é linearmente F-representável e N é um menor de M, então N é linearmente F-representável.

Concluíremos esta seção com alguns resultados importantes para a caracterização dos conjuntos independentes de menores. Tais resultados serão úteis para descrever certas noções semânticas da linguagem formal do próximo capítulo.

PROPOSIÇÃO II.3.6. [15, Proposição 3.1.8] Suponhamos que M seja uma matroide e que $X \subseteq E(M)$. Se B é uma base de $M \mid X$, então $\mathcal{I}(M / X) = \{ I \subseteq E(M) - X : I \cup B \in \mathcal{I}(M) \}$.

Demonstração. Suponhamos que $I \subseteq E(M) - X$ seja tal que $I \cup B \in \mathcal{I}(M)$. Temos $r_M(I \cup B) = r_M(I \cup X)$. Da Proposição II.3.3, obtemos:

$$\begin{aligned} r_{M/X}(I) &= r_M(I \cup X) - r_M(X) \\ &= r_M(I \cup B) - r_M(B) \\ &= |I \cup B| - |B| \\ &= |I|. \end{aligned}$$

Por outro lado, se $r_{M/X}(I) = |I|$, então $|I| + |B| = r_M(I \cup B)$. Disto, vemos que $r_M(I \cup B) = |I \cup B|$. Concluímos assim que $\mathcal{I}(M / X) = \{ I \subseteq E(M) - X : I \cup B \in \mathcal{I}(M) \}$. ⊣

É natural que o resultado seguinte à caracterização dos conjuntos independentes de uma contração de uma matroide seja a caracterização das bases desta contração. Tal caracterização é apresentada na Proposição II.3.7, que é uma consequência direta da propriedade de aumento dos conjuntos independentes e da Proposição II.3.6.

PROPOSIÇÃO II.3.7. [15, Corolário 3.1.9] Suponhamos que M seja uma matroide e que $X \subseteq E(M)$. Se B é uma base de $M \mid X$, então $\mathcal{B}(M / X) = \{ A \subseteq E(M) - X : A \cup B \in \mathcal{B}(M) \}$[m].

Usando a Proposição II.3.7, podemos demonstrar o seguinte resultado que será utilizado na prova do Lema II.3.9:

LEMA II.3.8. Suponhamos que M seja uma matroide. Dados $X, Y \subseteq E(M)$ se X é uma base de $M \mid Y$, então todo elemento de $Y - X$ é um loop de M / X.

Demonstração. Suponhamos que exista $a \in Y - X$ que não seja um loop de M / X. Nesse caso existe $A \in \mathcal{B}(M / X)$ tal que $a \in A$. Da Proposição II.3.7, vemos que $B = A \cup X$ é uma base de M. Como $a \in Y - X$ e $X \cup a \subseteq B$, vemos que $X \cup a \subseteq Y$ é independente, o que contradiz a $\subseteq$-maximalidade de X em $\mathcal{I}(M \mid Y)$. ⊣

O Lema II.3.9 permitirá escrever um menor de uma matroide de maneira especial e isto facilitará a caracterização dos conjuntos dependentes de um menor na Proposição II.3.11.

LEMA II.3.9. [15, Lema 3.3.5] Suponhamos que M seja uma matroide e que $X, Y \subseteq E(M)$ sejam disjuntos. Se Y_1 é uma base de $M \mid Y$ e X_1 é uma base de $M^* \mid X$, então para toda partição (X_2, Y_2) de $(X - X_1) \cup (Y - Y_1)$ vale $M \setminus X / Y = M \setminus (X_1 \cup Y_2) / (Y_1 \cup X_2)$.

Demonstração. Do Lema II.3.8, vemos que todo elemento de $Y - Y_1$ é um loop de M / Y_1. Se (W_1, W_2) é uma partição de $Y - Y_1$, então podemos escrever $Y = (Y_1 \cup W_1) \cup W_2$ com $(Y_1 \cup W_1) \cap W_2 = \emptyset$. Disto, obtemos $M/Y = M/(Y_1 \cup W_1) \setminus W_2$. Do Lema II.3.8, vemos que todo elemento de $X - X_1$ é um loop de M^* / X_1. Se (Z_1, Z_2) é uma partição de $X - X_1$, então podemos escrever $X = (X_1 \cup Z_1) \cup Z_2$ com $(X_1 \cup Z_1) \cap Z_2 = \emptyset$. Disto, obtemos $M^* / X = M^* / (X_1 \cup Z_1) \setminus Z_2$. Segue então que $M \setminus X = M \setminus (X_1 \cup Z_1) / Z_2$. Da Proposição II.3.4, obtemos $M \setminus X / Y = M \setminus (X_1 \cup Z_1 \cup W_2) / (Y_1 \cup W_1 \cup Z_2)$. Como $(Z_1 \cup W_2, W_1 \cup Z_2)$ é uma partição de $(X - X_1) \cup (Y - Y_1)$, obtemos o resultado desejado. ⊣

[m] Em outras palavras, as bases de M / X são obtidas das diferenças das bases de M pelas bases de $M \mid X$.

O Teorema II.3.10 permitirá escrever todo menor de uma matroide M na forma $M \setminus I^* / I$, onde $I^* \in \mathcal{I}(M^*)$ e $I \in \mathcal{I}(M)$ são disjuntos.

TEOREMA II.3.10 (Menores). [15, Proposição 3.3.6] Suponhamos que M seja uma matroide e que $X, Y \subseteq E(M)$ sejam disjuntos. Se Y_1 é uma base de $M \mid Y$ e X_1 é uma base de $M^* \mid X$, então

$$M \setminus X / Y = M \setminus [X_1 \cup (Y - Y_1)] / [Y_1 \cup (X - X_1)]$$

com $X_1 \cup (Y - Y_1) \in \mathcal{I}(M^*)$ e $Y_1 \cup (X - X_1) \in \mathcal{I}(M)$.

Demonstração. O primeiro resultado segue do Lema II.3.9. Do Lema II.3.8, sabemos que se $a \in Y - Y_1$, então a é um loop de M / Y_1. Disto, vemos que a é um coloop de $M^* \setminus Y_1$, e portanto, $Y - Y_1$ é independente em M^*. Sabemos que X_1 é uma base de $M^* \mid X$, e portanto, X_1 é independente em M^*. Existe $B^* \in \mathcal{B}(M^*)$ tal que $X_1 \cup (Y - Y_1) \subseteq B^*$, e assim, $X_1 \cup (Y - Y_1) \in \mathcal{I}(M^*)$. Raciocínio análogo para $Y_1 \cup (X - X_1) \in \mathcal{I}(M)$. ⊣

Uma caracterização dos conjuntos dependentes de menores é apresentada pela seguinte Proposição II.3.11. Este resultado será útil para provar a Proposição III.2.9 da Seção III.2.

PROPOSIÇÃO II.3.11. Suponhamos que M seja uma matroide, que $I^* \in \mathcal{I}(M^*)$ e $I \in \mathcal{I}(M)$ sejam disjuntos, que N seja uma matroide e que φ seja um isomorfismo de N em $M \setminus I^* / I$. Um conjunto $X \subseteq E(N)$ é dependente em N sse existe $Y \subseteq E(M)$ dependente em M tal que $Y - \varphi[X] \subseteq I$.

Demonstração. Se $X \notin \mathcal{I}(N)$, então basta tomar $Y = \varphi[X]$. Provemos a outra condicional. Suponhamos que $X \in \mathcal{I}(N)$ e que exista $Y \subseteq E(M)$ dependente em M tal que $Y - \varphi[X] \subseteq I$. De $N \cong M \setminus I^* / I$, vemos que $\varphi[X] \subseteq E(M / I) - I^*$ é tal que $\varphi[X] \in \mathcal{I}(M / I)$. Da Proposição II.3.6, segue $\varphi[X] \cup I \in \mathcal{I}(M)$. Temos $Y - \varphi[X] \subseteq I$ e $\varphi[X] \cap Y \subseteq \varphi[X]$. Disto, vemos que $Y \subseteq \varphi[X] \cup I$, o que contradiz Y ser dependente em M. ⊣

II.4 AMÁLGAMAS PRÓPRIAS

Até o momento, vimos que matroides podem ser caracterizadas de muitas maneiras diferentes e que a teoria admite um princípio de dualidade. Apresentaremos nesta seção uma construção de matroides que será muito útil para os nossos propósitos. O Teorema II.4.13 é um resultado fundamental para o trabalho, uma vez que ele caracteriza os conjuntos independentes dessa construção de matroide. Esta caracterização será importante para provar resultados do próximo capítulo. As referências principais desta seção são J. Oxley [15] e D. Mayhew, M. Newman e G. Whittle [12].

Ao longo desta seção, vamos supor que $M_1 = (E_1, \mathcal{I}_1)$, $M_2 = (E_2, \mathcal{I}_2)$ e $L = (T, \mathcal{I}(L))$ são matroides simples tais que $M_1 \mid T = M_2 \mid T = L$ e $T = E_1 \cap E_2$ e vamos denotar $E = E_1 \cup E_2$. Também ao longo da seção, denotaremos por r_i, cl_i, $\mathcal{C}_i$, $\mathcal{B}_i$ e $\mathcal{F}_i$ a função posto, o operador de fecho, a coleção dos circuitos, a coleção das bases e a coleção de flats da matroide M_i, respectivamente, para cada $i \in \{1, 2\}$. Não vamos nos preocupar em fornecer exemplos para as construções de matroides desta seção, pois veremos construções sistemáticas de vários exemplos especiais na Seção II.5.

Dizemos que uma matroide $U = (E, \mathcal{I}(U))$ é uma *amálgama* de M_1 e M_2 quando $U \mid E_1 = M_1$ e $U \mid E_2 = M_2$. Vide a Figura II.4.1 interpretando as setas como restrições de matroides. Ao longo da seção, vamos reservar o símbolo U para simbolizar uma amálgama de M_1 e M_2. Uma *amálgama livre* de M_1 e M_2 é uma amálgama U de M_1 e M_2 tal que todo conjunto independente de uma amálgama de M_1 e M_2 é independente em U. Em outras palavras, se V é uma amálgama de M_1 e M_2 e U é a amálgama livre de M_1 e M_2, então $\mathcal{I}(V) \subseteq \mathcal{I}(U)$. Observemos que se $X \cap E_i \notin \mathcal{I}_i$ para algum $i \in \{1, 2\}$, então $X \subseteq E$ não pode ser independente em uma amálgama de M_1 e M_2.

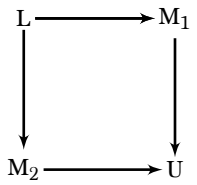

Figura II.4.1: O diagrama da figura ilustra a propriedade de amálgama. Cada seta indica que a matroide origem é uma restrição da matroide destino.

Vamos definir a seguir duas funções η e ζ cujos propósitos ficarão claros quando estabelecermos a Proposição II.4.2 mais adiante, pois nosso intuito é conectar tais funções com a função posto de um tipo especial de amálgama livre. Definamos a função $\eta : 2^E \longrightarrow \mathbb{N}$ pondo

$$\eta(X) = r_1(X \cap E_1) + r_2(X \cap E_2) - r_L(X \cap T)$$

para cada $X \subseteq E$. Se U é uma amálgama de M_1 e M_2, então segue da submodularidade da função posto de U que $r_U(X) \leq \eta(X)$. Definamos a função $\zeta : 2^E \longrightarrow \mathbb{N}$ pondo

$$\zeta(X) = \min\{\, \eta(Y) : X \subseteq Y \subseteq E \,\} \tag{II.1}$$

para cada $X \subseteq E$. O seguinte lema mostra que a função ζ tem as primeiras duas propriedades de uma função posto de uma matroide.

LEMA II.4.1. A função ζ satisfaz o seguinte:

(1) Se $X \subseteq E$, então $\zeta(X) \leq |X|$.

(2) Se $X \subseteq Y \subseteq E$, então $\zeta(X) \leq \zeta(Y)$.

Demonstração.

(1) Basta mostrar que $\eta(X) \leq |X|$. Suponhamos que B seja uma base de $L \mid X \cap T$. Para cada $i \in \{1, 2\}$, o conjunto B é independente em $M_i \mid X \cap E_i$, e assim, podemos estendê-lo em $M_i \mid X \cap E_i$ para uma de suas bases B_i de modo que $B_1 \cap B_2 = B$. Disto, obtemos

$$\begin{aligned}
\eta(X) &= r_1(X \cap E_1) + r_2(X \cap E_2) - r_L(X \cap T) \\
&= |B_1| + |B_2| - |B| \\
&= |B_1 \cup B_2| \\
&\leq |X|.
\end{aligned}$$

Da Equação II.1, obtemos $\zeta(X) \leq |X|$.

(2) Da Equação II.1, segue que existe $Z \subseteq E$ com $Y \subseteq Z$ tal que $\zeta(Y) = \eta(Z)$. Da hipótese $X \subseteq Y$, obtemos $X \subseteq Z$, e portanto, $\zeta(X) \leq \eta(Z) = \zeta(Y)$. ⊣

A Proposição II.4.2 a seguir mostra que se ζ for submodular, então ela é na verdade a função posto da amálgama livre de M_1 e M_2.

PROPOSIÇÃO II.4.2. [15, Proposição 12.4.2] Se ζ é submodular, então ζ é a função posto da amálgama livre de M_1 e M_2. Neste caso, dizemos que esta matroide é a *amálgama própria* de M_1 e M_2 e a denotamos por $M_1 \oplus_L M_2$.

Demonstração. Suponhamos que ζ seja submodular. Do Teorema II.2.12, segue que ζ é a função posto de uma matroide V sobre E. Se U é uma amálgama de M_1 e M_2 e $I \in \mathcal{I}(U)$, então segue da Equação II.1 que existe $Y \subseteq E$ tal que $I \subseteq Y$ e $\zeta(I) = \eta(Y)$. Temos $|I| = r_U(I) \leq r_U(Y) \leq \eta(Y) = \zeta(I)$. Isto mostra que $I \in \mathcal{I}(V)$. ⊣

Denotemos por $\mathcal{L}(M_1, M_2)$ a coleção dos subconjuntos $X \subseteq E$ tais que $X \cap E_i \in \mathcal{F}_i$ para cada $i \in \{1, 2\}$. Observemos que, como $\mathcal{F}_1$ e $\mathcal{F}_2$ são fechados para interseção, então $\mathcal{L}(M_1, M_2)$ também é fechado para interseção. Segue da definição de fecho que se M é uma matroide e $X \subseteq Y \subseteq E(M)$, então $cl_{M|Y}(X) = cl_M(X)$. Disto, vemos que $cl_i(X \cap E_i) \subseteq cl_U(X) \cap E_i$. Denotemos por $\mathcal{F}(U)$ a coleção dos flats de U.

LEMA II.4.3. $\mathcal{F}(U) \subseteq \mathcal{L}(M_1, M_2)$.

Demonstração. Dado $F \in \mathcal{F}(U)$, temos $F = cl_U(F)$. Dado $i \in \{1, 2\}$, obtemos $cl_i(F \cap E_i) \subseteq cl_U(F) \cap E_i = F \cap E_i$, e portanto, $F \cap E_i \in \mathcal{F}_i$. Assim, $F \in \mathcal{L}(M_1, M_2)$. ⊣

Definamos a função $\Phi : 2^E \longrightarrow \mathcal{L}(M_1, M_2)$ pondo

$$\Phi(X) = cl_1(X \cap E_1) \cup cl_2(X \cap E_2)$$

para cada $X \subseteq E$. Dado $X \in \mathcal{L}(M_1, M_2)$, temos $X \cap E_1 = cl_1(X \cap E_1)$ e $X \cap E_2 = cl_2(X \cap E_2)$, e assim, $\Phi(X) = X$. Observemos que para todos X, $Y \in \mathcal{L}(M_1, M_2)$ sempre vale $X \cap \Phi(X \cup Y) = X$. Dado $X \subseteq E$, definamos $\overline{X}$ como a interseção de todos os elementos de $\mathcal{L}(M_1, M_2)$ que contém X. Observemos que, como $\mathcal{L}(M_1, M_2)$ é fechado para a interseção, então $\overline{X}$ pertence à coleção $\mathcal{L}(M_1, M_2)$. O Lema II.4.4 detalha o Lema 12.4.6 feito por J. Oxley [15], que mostra que o valor da função ζ avaliada em $X \subseteq E$ pode ser obtido avaliando a função η nos elementos de $\mathcal{L}(M_1, M_2)$ que contém X.

LEMA II.4.4. [15, Lema 12.4.6] Dado $X \subseteq E$, vale $\zeta(X) = \min\{ \eta(Y) : X \subseteq Y \in \mathcal{L}(M_1, M_2) \}$.

Demonstração. Definamos as funções $\phi_1, \phi_2 : 2^E \longrightarrow 2^E$ dadas por

$$\phi_1(X) = cl_1(X \cap E_1) \cup (X \cap E_2)$$
$$\phi_2(X) = (X \cap E_1) \cup cl_2(X \cap E_2).$$

Segue de $X = (X \cap E_1) \cup (X \cap E_2)$ que $X \subseteq \phi_1(X)$ e $X \subseteq \phi_2(X)$. Observemos também que $\phi_1(X) \cup \phi_2(X) = \Phi(X)$. Disto, segue que um subconjunto de E é ponto fixo de ϕ_1 e ϕ_2 sse é ponto fixo de Φ.

Afirmação 1. Tomemos $\{ i, j \} = \{ 1, 2 \}$. Dado $X \subseteq E$, valem:

(1) $\phi_i(X) \cap E_j = (\phi_i(X) \cap T) \cup (X \cap E_j)$.

(2) $X \cap T \subseteq (\phi_i(X) \cap T) \cap (X \cap E_j)$.

(3) $r_i(\phi_i(X) \cap E_i) = r_i(X \cap E_i)$.

(4) $\eta(\phi_i(X)) \leq \eta(X)$.

Demonstração. Dado $X \subseteq E$ valem:

(1) $\begin{aligned}\phi_i(X) \cap E_j &= (\mathrm{cl}_i(X \cap E_i) \cap E_j) \cup (X \cap E_j)\\ &= (\mathrm{cl}_i(X \cap E_i) \cap T) \cup (X \cap E_j)\\ &= (\mathrm{cl}_i(X \cap E_i) \cap T) \cup (X \cap T) \cup (X \cap E_j)\\ &= [(\mathrm{cl}_i(X \cap E_i) \cup (X \cap E_j)) \cap T] \cup (X \cap E_j)\\ &= (\phi_i(X) \cap T) \cup (X \cap E_j).\end{aligned}$

(2) $\begin{aligned}(X \cap T) \cap (\phi_i(X) \cap E_j) &= (X \cap T) \cap [(\phi_i(X) \cap T) \cup (X \cap E_j)]\\ &= [(\phi_i(X) \cap X) \cap T] \cup (X \cap T)\\ &= X \cap T.\end{aligned}$

(3) $\begin{aligned}r_i(\phi_i(X) \cap E_i) &= r_i((\mathrm{cl}_i(X \cap E_i) \cap E_i) \cup (X \cap T))\\ &= r_i(\mathrm{cl}_i(X \cap E_i) \cap E_i)\\ &= r_i(\mathrm{cl}_i(X \cap E_i))\\ &= r_i(X \cap E_i).\end{aligned}$

(4) Podemos supor que $i = 1$ e $j = 2$. Do primeiro e segundo itens, obtemos:

$$\begin{aligned}r_2(\phi_1(X) \cap E_2) + r_2(X \cap T) &= r_2((\phi_1(X) \cap T) \cup (X \cap E_2)) + r_2(X \cap T)\\ &\leq r_2((\phi_1(X) \cap T) \cup (X \cap E_2)) +\\ &\quad r_2((\phi_1(X) \cap T) \cap (X \cap E_2))\\ &\leq r_2(\phi_1(X) \cap T) + r_2(X \cap E_2).\end{aligned}$$

Disto e do terceiro item, obtemos:

$$\begin{aligned}\eta(\phi_1(X)) &= r_1(\phi_1(X) \cap E_1) + r_2(\phi_1(X) \cap E_2) - r_L(\phi_1(X) \cap T)\\ &\leq r_1(X \cap E_1) + r_2(\phi_1(X) \cap T) + r_2(X \cap E_2) -\\ &\quad r_2(X \cap T) - r_L(\phi_1(X) \cap T)\\ &= r_1(X \cap E_1) + r_2(X \cap E_2) - r_L(X \cap T)\\ &= \eta(X).\end{aligned}$$

⊣

Definamos $\phi : 2^E \longrightarrow 2^E$ pondo $\phi(X) = (\phi_2 \circ \phi_1)(X)$. Da Afirmação 1, temos $X \subseteq \phi_1(X) \subseteq \phi(X)$. Segue por indução que $\phi^m(X) \subseteq \phi^{m+1}(X)$ para todo $m \in \mathbb{N}$. A coleção $\{\, \phi^m(X) \subseteq E : m \in \mathbb{N} \,\}$ é finita e isto mostra que existe $m_0 \in \mathbb{N}$ tal que $\phi^{m_0+1}(X) = \phi^{m_0}(X)$. Tomemos $Y = \phi^{m_0}(X)$. Temos $\phi(Y) = Y$. Disto, segue $\Phi(Y) = Y$. Obtemos $Y \in \mathcal{L}(M_1, M_2)$ e $X \subseteq Y$, e portanto, $\overline{X} \subseteq Y$.

Afirmação 2. $Y = \overline{X}$.

Demonstração. Basta mostrar que $Y \subseteq \overline{X}$. De $\overline{X} \in \mathcal{L}(M_1, M_2)$, segue $\Phi(\overline{X}) = \overline{X}$. De $\overline{X}$ ser um ponto fixo de Φ, vemos que $\phi_1(\overline{X}) = \overline{X}$ e $\phi_2(\overline{X}) = \overline{X}$. Mais ainda, segue que $\phi(\overline{X}) = \overline{X}$. Sabemos que $X \subseteq \phi_1(X) \subseteq \overline{X}$ e $X \subseteq \phi_2(X) \subseteq \overline{X}$. Assim, $Y = \phi^{m_0}(X) \subseteq \phi^{m_0}(\overline{X}) = \overline{X}$. ⊣

Estamos prontos para finalizar a demonstração do lema. Suponhamos que $X \subseteq Z \subseteq E$ sejam tais que $\zeta(X) = \eta(Z)$. De maneira análoga ao que foi feito anteriormente, existe $n_0 \in \mathbb{N}$ tal que $\phi^{n_0}(Z) = \phi^{n_0+1}(Z)$. Tomemos $W = \phi^{n_0}(Z)$. Em virtude da Afirmação 2, vemos que $W = \overline{Z}$ e $W \in \mathcal{L}(M_1, M_2)$. Aplicando um número finito de vezes o resultado do último item da Afirmação 1, obtemos $\eta(W) \leq \eta(Z)$. De $Z \subseteq W$ e do segundo item do Lema II.4.1, obtemos $\eta(Z) \leq \eta(W)$. Isto mostra que $\zeta(X) = \eta(W)$, o que conclui a demonstração do lema. ⊣

COROLÁRIO II.4.5. Dados $X, Y \in \mathcal{L}(M_1, M_2)$, definamos $X \vee Y = \Phi(X \cup Y)$. Vale $\eta(X \vee Y) \leq \eta(X \cup Y)$.

Demonstração. Suponhamos que $X, Y \in \mathcal{L}(M_1, M_2)$ e tomemos $Z = X \cup Y$. Sabemos que $\overline{Z}$ é o ponto fixo de ϕ que contém Z. Da Afirmação 1 do Lema II.4.4, temos $S \subseteq \phi_1(S) \subseteq \phi(S)$ para cada $S \subseteq E$. Assim, $\overline{Z} \subseteq \phi_1(\overline{Z}) \subseteq \phi(\overline{Z}) = \overline{Z}$, e portanto, $\overline{Z} = \phi_1(\overline{Z})$. Disto, obtemos $\phi_2(\overline{Z}) = \phi_2(\phi_1(\overline{Z})) = \phi(\overline{Z}) = \overline{Z}$. Temos $\phi_1(\overline{Z}) = \overline{Z}$ e $\phi_2(\overline{Z}) = \overline{Z}$, e portanto, $\Phi(\overline{Z}) = \overline{Z}$. De $Z \subseteq \overline{Z}$ e $\Phi(Z) = \phi_1(Z) \cup \phi_2(Z)$, segue $\Phi(Z) \subseteq \overline{Z}$. Por outro lado, sabemos que $\overline{Z}$ é o menor elemento de $\mathcal{L}(M_1, M_2)$ que contém Z. Como $\Phi(Z) \in \mathcal{L}(M_1, M_2)$ e $\overline{Z} \subseteq \Phi(Z)$, vemos que $Z \subseteq \Phi(Z)$. Disto, segue que $\Phi(Z) = \overline{Z}$, e do último item da Afirmação 1, segue $\eta(X \vee Y) \leq \eta(X \cup Y)$. ⊣

Dada uma matroide M, definamos uma função $\Delta_M : 2^{E(M)} \times 2^{E(M)} \longrightarrow \mathbb{N}$ pondo

$$\Delta_M(X, Y) = r_M(X) + r_M(Y) - r_M(X \cup Y) - r_M(X \cap Y).$$

Quando $\Delta_M(X, Y) = 0$, dizemos que (X, Y) é um *par modular* de M. Uma matroide M é *modular* quando todo par de flats de M é modular. O Exemplo II.4.6 a seguir mostra que toda matroide simples de posto dois é modular.

EXEMPLO II.4.6 (Flats e Modularidade). Suponhamos que M seja uma matroide simples de posto dois. Se $|X| = 2$, então $X \in \mathcal{B}(M)$. De fato, suponhamos que $X \notin \mathcal{B}(M)$. Disto, segue que $X \notin \mathcal{I}(M)$ e $r_M(X) = 1$. Existe $Y \in \mathcal{I}(M)$ tal que $Y \subseteq X$ e $|Y| = 1$. Disto e de $|X| = 2$, obtemos $X - Y \in \mathcal{C}(M)$, o que contradiz a simplicidade de M. Se $F_1, F_2 \in \mathcal{F}(M)$, então $F_1 \subseteq F_2$ ou $F_2 \subseteq F_1$ ou $r_M(F_1) = r_M(F_2) = 1$. Isto mostra que M é modular. ⊣⊢

Uma função $\varphi : \mathcal{L}(M_1, M_2) \longrightarrow \mathbb{N}$ é submodular em $\mathcal{L}(M_1, M_2)$ quando satisfaz

$$\varphi(X \vee Y) + \varphi(X \cap Y) \leq \varphi(X) + \varphi(Y)$$

para todos $X, Y \in \mathcal{L}(M_1, M_2)$. A Proposição II.4.7 a seguir fornecerá condições suficientes para que a restrição $\eta \mid \mathcal{L}(M_1, M_2)$ seja submodular.

PROPOSIÇÃO II.4.7. [15, Proposição 12.4.9] Dados $X, Y \in \mathcal{L}(M_1, M_2)$, se

$$\Delta_L(X \cap T, Y \cap T) \leq \max\{\, \Delta_1(X \cap E_1, Y \cap E_1), \Delta_2(X \cap E_2, Y \cap E_2) \,\},$$

então a restrição $\eta \mid \mathcal{L}(M_1, M_2)$ é submodular.

Demonstração. Dados $X, Y \in \mathcal{L}(M_1, M_2)$, sabemos que $\eta(X \vee Y) \leq \eta(X \cup Y)$ em virtude do Corolário II.4.5. Disto, segue que $\eta(X) + \eta(Y) - \eta(X \vee Y) - \eta(X \cap Y) \geq \eta(X) + \eta(Y) - \eta(X \cup Y) - \eta(X \cap Y)$. Usando a hipótese, temos:

$$\begin{aligned}
\eta(X) + \eta(Y) - \eta(X \cup Y) - \eta(X \cap Y) &= r_1(X \cap E_1) + r_2(X \cap E_2) - r_L(X \cap T) \\
&\quad + r_1(Y \cap E_1) + r_2(Y \cap E_2) - r_L(Y \cap T) \\
&\quad - r_1((X \cup Y) \cap E_1) - r_2((X \cup Y) \cap E_2) \\
&\quad + r_L((X \cup Y) \cap T) - r_1((X \cap Y) \cap E_1) \\
&\quad - r_2((X \cap Y) \cap E_2) + r_L((X \cap Y) \cap T) \\
&= r_1(X \cap E_1) + r_1(Y \cap E_1) \\
&\quad - r_1((X \cup Y) \cap E_1) - r_1((X \cap Y) \cap E_1) \\
&\quad + r_2(X \cap E_2) + r_2(Y \cap E_2) \\
&\quad - r_2((X \cup Y) \cap E_2) - r_2((X \cap Y) \cap E_2) \\
&\quad - r_L(X \cap T) - r_L(Y \cap T) \\
&\quad + r_L((X \cup Y) \cap T) + r_L((X \cap Y) \cap T) \\
&= \Delta_1(X \cap E_1, Y \cap E_1) - \Delta_L(X \cap T, Y \cap T) \\
&\quad + \Delta_2(X \cap E_2, Y \cap E_2) \\
&\geq 0
\end{aligned}$$

Isto mostra que a restrição $\eta \mid \mathcal{L}(M_1, M_2)$ é submodular. ⊣

PROPOSIÇÃO II.4.8. [15, Proposição 12.4.7] Se a restrição $\eta \mid \mathcal{L}(M_1, M_2)$ é submodular, então ζ é submodular.

Demonstração. Dados $X, Y \subseteq E$, segue do Lema II.4.4 que existem $A \in \mathcal{L}(M_1, M_2)$ com $X \subseteq A$ e $B \in \mathcal{L}(M_1, M_2)$ com $Y \subseteq B$ tais que $\zeta(X) = \eta(A)$ e $\zeta(Y) = \eta(B)$. Como $X \subseteq A$ e $Y \subseteq B$, vemos que $X \cap Y \subseteq A \cap B$ e $X \cup Y \subseteq A \vee B$. Do Lema II.4.1, sabemos que $\zeta(X \cap Y) \leq \zeta(A \cap B)$ e $\zeta(X \cup Y) \leq \zeta(A \vee B)$. Assim:

$$\begin{aligned}
\zeta(X \cup Y) + \zeta(X \cap Y) &\leq \zeta(A \vee B) + \zeta(A \cap B) \\
&\leq \eta(A \vee B) + \eta(A \cap B) \\
&\leq \eta(A) + \eta(B) \\
&= \zeta(X) + \zeta(Y).
\end{aligned}$$ ⊣

Observemos que se $F \in \mathcal{F}_i$, então $F \cap T \in \mathcal{F}(L)$. Os resultados provados até aqui são suficientes para provar o Teorema II.4.9 e ele fornecerá condições suficientes para a existência de amálgamas próprias.

TEOREMA II.4.9 (Existência da Amálgama Própria). [15, Teorema 12.4.10] Se L é modular, então existe a amálgama própria $M_1 \oplus_L M_2$.

Demonstração. Tomemos $i \in \{1, 2\}$. Se L é modular, então $\Delta_L(F_1, F_2) = 0$ para todos $F_1, F_2 \in \mathcal{F}(L)$. Dados $X, Y \subseteq \mathcal{L}(M_1, M_2)$, sabemos que $X \cap E_i, Y \cap E_i \in \mathcal{F}_i$ para cada $i \in \{1, 2\}$, e portanto, $X \cap T, Y \cap T \in \mathcal{F}(L)$. Disto, segue $\Delta_L(X \cap T, Y \cap T) = 0$. Da Proposição II.4.7, vemos que a restrição $\eta \mid \mathcal{L}(M_1, M_2)$ é submodular. Da Proposição II.4.8, segue que a função ζ é submodular. Da Proposição II.4.2, vemos que ζ é a função posto de $M_1 \oplus_L M_2$. ⊣

COROLÁRIO II.4.10. [15, Exercício 5(i) sec. 12.4] Suponhamos que L seja modular e que $U = M_1 \oplus_L M_2$ seja a amálgama própria de M_1 e M_2. Temos $\mathcal{F}(M_1 \oplus_L M_2) = \mathcal{L}(M_1, M_2)$ e

$$\begin{aligned} cl_U(X) &= \Phi(X) \\ &= cl_1(X \cap E_1) \cup cl_2(X \cap E_2). \end{aligned}$$

Demonstração. Primeiro, vamos mostrar que Φ possui as propriedades apresentadas na Proposição II.2.14.

Afirmação 1. A função Φ satisfaz:

(1) Dados $X, Y \subseteq E$, temos $X \subseteq \Phi(Y)$ sse $\Phi(X) \subseteq \Phi(Y)$.

(2) Dados $X \subseteq E$ e $a, b \in E$, se $a \in \Phi(X \cup b) - \Phi(X)$, então $b \in \Phi(X \cup a)$.

Demonstração.

(1) Dados $X, Y \subseteq E$, se $X \subseteq \Phi(Y)$, então $\Phi(X) \subseteq \Phi(\Phi(Y)) = \Phi(Y)$. Disto, temos $X \subseteq \Phi(Y)$ sse $\Phi(X) \subseteq \Phi(Y)$.

(2) Dados $X \subseteq E$ e $a, b \in E$, suponhamos que $a \in \Phi(X \cup b) - \Phi(X)$. Temos $\Phi(X \cup b) = [cl_1((X \cup b) \cap E_1) \cup cl_2((X \cup b) \cap E_2)] - [cl_1(X \cap E_1) \cup cl_2(X \cap E_2)]$. Disto, vemos que $a \in cl_i((X \cup b) \cap E_i)$ para algum $i \in \{1, 2\}$, e assim, $a \in cl_i((X \cup b) \cap E_i) - cl_i(X \cap E_i)$. Disto e da Proposição II.2.14, vemos que $b \in cl_i(X \cup a)$, e portanto, $b \in \Phi(X \cup a)$. ⊣

Do Teorema II.2.15, segue que existe uma matroide V sobre E cujo operador de fecho é Φ. Sabemos que $\Phi(X) \subseteq cl_U(X)$. Suponhamos que exista $I \in \mathcal{I}(U)$ tal que $I \notin \mathcal{I}(V)$. De $I \in \mathcal{I}(U)$, segue que para todo $a \in I$ vale $a \notin cl_U(I - a)$. De $I \notin \mathcal{I}(V)$, segue que existe $b \in I$ tal que $b \in \Phi(I - b)$. De $\Phi(I - b) \subseteq cl_U(I - b)$, obtemos $b \in cl_U(I - b)$, o que é uma contradição. Isso estabelece a validade de $\mathcal{I}(U) \subseteq \mathcal{I}(V)$. Como U é a amálgama livre de M_1 e M_2, vemos que $U = V$. ⊣

COROLÁRIO II.4.11. [15, Exercício 5(ii) sec. 12.4] Suponhamos que L seja modular e que $U = M_1 \oplus_L M_2$ seja a amálgama própria de M_1 e M_2. A função posto desta matroide é

$$r_U(X) = r_1(X \cap E_1) + r_2(X \cap E_2) - r_L(cl_U(X) \cap T).$$

Demonstração. Do Lema II.4.4, segue que $r_U(X) = \eta(\overline{X})$. Da Afirmação 1 do Lema II.4.4, temos $Y \subseteq \phi_1(Y) \subseteq \phi(Y)$ para cada $Y \subseteq E$. Assim, $\overline{X} \subseteq \phi_1(\overline{X}) \subseteq \phi(\overline{X}) = \overline{X}$, e portanto, $\phi_1(\overline{X}) = \overline{X}$. Disto, obtemos $\phi_2(\overline{X}) = \phi_2(\phi_1(\overline{X})) = \phi(\overline{X}) = \overline{X}$. Sabemos que $\Phi(Y) = \phi_1(Y) \cup \phi_2(Y)$ para cada $Y \subseteq E$. Temos $\phi_1(\overline{X}) = \overline{X}$ e $\phi_2(\overline{X}) = \overline{X}$, e portanto, $\Phi(\overline{X}) = \overline{X}$. De $X \subseteq \overline{X}$ e $\Phi(Y) = \phi_1(Y) \cup \phi_2(Y)$ para cada $Y \subseteq E$, segue $\Phi(X) \subseteq \Phi(\overline{X}) = \overline{X}$. Por definição, $\overline{X}$ é a interseção de todos os elementos de $\mathcal{L}(M_1, M_2)$ que contém X. Disto, obtemos $\overline{X} \subseteq \Phi(X)$. Do Corolário II.4.10, temos $cl_U(X) = \Phi(X) = \overline{X}$. Isto mostra que $r_U(X) = \eta(cl_U(X))$.

Afirmação 1. Valem $r_1(cl_U(X) \cap E_1) = r_1(X \cap E_1)$ e $r_2(cl_U(X) \cap E_2) = r_2(X \cap E_2)$.

Demonstração. Tomemos $Y = \mathrm{cl}_U(X)$. Vamos mostrar que se B_1 é uma base de $M \mid X \cap E_1$, então B_1 é uma base de $M \mid Y \cap E_1$. Suponhamos que exista $a \in (Y \cap E_1) - (X \cap E_1) = (Y - X) \cap E_1$ tal que $r_1(B_1 \cup a) = |B_1| + 1$. De $a \in Y - X$, segue que existe $C \in \mathcal{C}(U)$ tal que $a \in C$ e $C \subseteq B_1 \cup a$. Temos $a \in E_1$ e $B_1 \subseteq E_1$, e portanto, $C \subseteq E_1$. Neste caso, vemos que $C \in \mathcal{C}_1$, o que mostra que $r_1(B_1 \cup a) = |B_1|$. Disto tudo, obtemos $0 = 1$, o que é uma contradição. Concluímos que para todo $a \in (Y - X) \cap E_1$ vale $r_1(B_1 \cup a) = |B_1|$. Isto mostra que toda base de $M \mid X \cap E_1$ é uma base de $M \mid Y \cap E_1$. Um raciocínio análogo mostra que toda base de $M \mid X \cap E_2$ é uma base de $M \mid Y \cap E_2$. ⊣

De $r_U(X) = \eta(\mathrm{cl}_U(X)) = r_1(\mathrm{cl}_U(X) \cap E_1) + r_2(\mathrm{cl}_U(X) \cap E_2) - r_L(\mathrm{cl}_L(X) \cap T)$ e da Afirmação 1, obtemos $r_U(X) = r_1(X \cap E_1) + r_2(X \cap E_2) - r_L(\mathrm{cl}_U(X) \cap T)$, como queríamos. ⊣

Da caracterização da função posto da amálgama própria dada pelo Corolário II.4.11, podemos provar o seguinte resultado. Ele generaliza uma parte dos resultados sobre amálgamas próprias provados por D. Mayhew, M. Newman e G. Whittle [12], uma vez que não assumimos hipóteses adicionais sobre a matroide L além de sua modularidade.

COROLÁRIO II.4.12. Suponhamos que L seja modular e que $U = M_1 \oplus_L M_2$ seja a amálgama própria de M_1 e M_2. Se $X \subseteq E$ é tal que $X \cap E_1 \in \mathcal{I}_1$ e $X \cap E_2 \in \mathcal{I}_2$, então $X \notin \mathcal{I}(U)$ caso valha alguma das afirmações a seguir:

(1) $T \subseteq \mathrm{cl}_1(X \cap E_1)$ e $r_2((X - E_1) \cup T) < r_2(X - E_1) + r(L)$.

(2) $T \subseteq \mathrm{cl}_2(X \cap E_2)$ e $r_1((X - E_2) \cup T) < r_1(X - E_2) + r(L)$.

(3) Existe $a \in T$ tal que $a \in \mathrm{cl}_1(X - E_2) \cap \mathrm{cl}_2(X - E_1)$.

Demonstração.

(1) Se $T \subseteq \mathrm{cl}_1(X \cap E_1)$, então $r_1((X \cap E_1) \cup T) = r_1(X \cap E_1)$. Temos $(X \cap E_2) \cup T = (X - E_1) \cup T$. Sabemos que $r_L(\mathrm{cl}_U(X \cup T) \cap T) = r(L)$. Disto, vemos que:

$$\begin{aligned} r_U(X) &\leq r_U(X \cup T) \\ &= r_1((X \cup T) \cap E_1) + r_2((X \cup T) \cap E_2) - r_L(\mathrm{cl}_U(X \cup T) \cap T) \\ &= r_1((X \cap E_1) \cup T) + r_2((X \cap E_2) \cup T) - r(L) \\ &< r_1((X \cap E_1) \cup T) + r_2(X - E_1) + r(L) - r(L) \\ &= r_1(X \cap E_1) + r_1(X - E_1) \\ &= |X \cap E_1| + |X - E_1| \\ &= |X|. \end{aligned}$$

Isto mostra que $X \notin \mathcal{I}(U)$.

(2) Análogo ao item anterior.

(3) Tomemos $\{i, j\} = \{1, 2\}$. De $a \in T$ e $a \in \mathrm{cl}_1(X - E_2) \cap \mathrm{cl}_2(X - E_1)$, vemos que $a \notin X$, pois caso contrário, teríamos $a \in X \cap T \subseteq X \cap E_i$ e isto contradiria $X \cap E_i \in \mathcal{I}_i$. De $a \in \mathrm{cl}_i(X - E_j)$, vemos que existe $C_i \in \mathcal{C}_i$ tal que $a \in C_i$ e $C_i \subseteq (X - E_j) \cup a$. Disto, obtemos $C_i, C_j \in \mathcal{C}(U)$ com $a \in C_i \cap C_j$ e $C_i \neq C_j$ tais que $C_i \cup C_j \subseteq X \cup a$. Da propriedade de eliminação, vemos que existe $C \in \mathcal{C}(U)$ tal que $C \subseteq (C_i \cup C_j) - a \subseteq X$. Isto mostra que $X \notin \mathcal{I}(U)$. ⊣

O Teorema II.4.13 a seguir caracteriza os conjuntos independentes da amálgama própria $U = M_1 \oplus_L M_2$, onde $L \cong U_{2,5}$ (Vide Exemplo II.2.10). Tal teorema desempenhará um papel fundamental nas demonstrações dos Teoremas II.5.14 e II.5.15 e do Teorema III.5.3.

TEOREMA II.4.13 (Conjuntos Dependentes da Amálgama Própria). [12, Proposição 4.1] Suponhamos $L \cong U_{2,5}$, que $U = M_1 \oplus_L M_2$ seja a amálgama própria de M_1 e M_2 e que $X \subseteq E$. Valem os seguintes resultados:

(1) Se $X \cap E_1 \notin \mathcal{I}_1$ ou $X \cap E_2 \notin \mathcal{I}_2$, então $X \notin \mathcal{I}(U)$.

(2) Se $X \cap E_1 \in \mathcal{I}_1$ e $X \cap E_2 \in \mathcal{I}_2$, então $X \notin \mathcal{I}(U)$ sse vale alguma das afirmações:

(2.1) $T \subseteq \mathrm{cl}_1(X \cap E_1)$ e $r_2((X - E_1) \cup T) < r_2(X - E_1) + 2$.

(2.2) $T \subseteq \mathrm{cl}_2(X \cap E_2)$ e $r_1((X - E_2) \cup T) < r_1(X - E_2) + 2$.

(2.3) Existe $a \in T$ tal que $a \in \mathrm{cl}_1(X - E_2) \cap \mathrm{cl}_2(X - E_1)$.

Demonstração. Em virtude do Corolário II.4.12, basta que provemos o outro sentido da condicional para estabelecer o segundo resultado. Dado $X \subseteq E$, suponhamos que $X \notin \mathcal{I}(U)$ seja tal que $X \cap E_1 \in \mathcal{I}(M)$ e $X \cap E_2 \in \mathcal{I}(N)$. Temos $X \nsubseteq E_1$ e $X \nsubseteq E_2$. Existe $Y_0 \subseteq E$ minimal pela inclusão tal que $X \subseteq Y_0$ e $\eta(Y_0) < |X|$. Escrevamos $Y_0 = X \cup A$ com $X \cap A = \emptyset$. De $X \cap E_1 \in \mathcal{I}_1$ e $X \cap E_2 \in \mathcal{I}_2$, segue que $A \neq \emptyset$. Da $\subseteq$-minimalidade de Y_0, vemos que $A \subseteq \mathrm{cl}_U(X)$, e portanto, $\mathrm{cl}_U(Y_0) = \mathrm{cl}_U(X)$. Disto, obtemos $r_U(Y_0) = r_U(X)$. A Afirmação 1 a seguir mostra que $A \subseteq T$.

Afirmação 1. Valem $Y_0 \subseteq X \cup E_1$ e $Y_0 \subseteq X \cup E_2$.

Demonstração. De fato, suponhamos que para algum $i \in \{1, 2\}$ exista $a \in Y_0 - (X \cup E_i)$. Observemos que $Y_0 - (X \cup E_i) \subseteq Y_0 - (X \cup T)$. Temos então $r_L((Y_0 - a) \cap T) = r_L(Y_0 \cap T)$. Da submodularidade do posto, vemos que

$$\begin{aligned} \eta(Y_0 - a) &= r_1((Y_0 - a) \cap E_1) + r_2((Y_0 - a) \cap E_2) - r_L((Y_0 - a) \cap T) \\ &\leq r_1(Y_0 \cap E_1) + r_2(Y_0 \cap E_2) - r_L(Y_0 \cap T) \\ &= \eta(Y_0), \end{aligned}$$

e portanto, $Y_0 - a \subseteq E$ é tal que $X \subseteq Y_0 - a$ e $\eta(Y_0 - a) < |X|$, o que contradiz a $\subseteq$-minimalidade de Y_0. ⊣

A Afirmação 2 a seguir permite que escrevamos $A \cap \mathrm{cl}_L(X \cap T) = \emptyset$. De fato, se existe $a \in A \cap \mathrm{cl}_L(X \cap T)$, então $a \in \mathrm{cl}_L(X \cap T) \subseteq \mathrm{cl}_L((Y_0 - a) \cap T)$, o que é uma contradição. Disto, vemos que $Y_0 \cap T \in \mathcal{I}(L)$ e que $Y_0 \cap E_1 \notin \mathcal{I}(M)$ e $Y_0 \cap E_2 \notin \mathcal{I}(N)$.

Afirmação 2. Para todo $a \in Y_0 \cap T$, temos $a \notin \mathrm{cl}_L((Y_0 - a) \cap T)$ e $a \in \mathrm{cl}_1((Y_0 - a) \cap E_1) \cap \mathrm{cl}_2((Y_0 - a) \cap E_2)$.

Demonstração. Se $a \in \mathrm{cl}_L((Y_0 - a) \cap T)$, então $r_L(Y_0 \cap T) = r_L(((Y_0 - a) \cap T) \cup a) = r_L((Y_0 - a) \cap T)$. Disto e de $\eta(Y_0) < \eta(Y_0 - a)$, segue que

$$\begin{aligned} r_1(Y_0 \cap E_1) + r_2(Y_0 \cap E_2) &< r_1((Y_0 - a) \cap E_1) + r_2((Y_0 - a) \cap E_2) \\ &\leq r_1(Y_0 \cap E_1) + r_2(Y_0 \cap E_2), \end{aligned}$$

o que é uma contradição. Agora, se $a \notin \mathrm{cl}_1((\mathrm{Y}_0 - a) \cap \mathrm{E}_1)$ e $a \in \mathrm{cl}_2((\mathrm{Y}_0 - a) \cap \mathrm{E}_2)$, então $r_1(\mathrm{Y}_0 \cap \mathrm{E}_1) = r_1(((\mathrm{Y}_0 - a) \cap \mathrm{E}_1) \cup a) = r_1((\mathrm{Y}_0 - a) \cap \mathrm{E}_1) + 1$ e $r_2(\mathrm{Y}_0 \cap \mathrm{E}_2) = r_\mathrm{N}(((\mathrm{Y}_0 - a) \cap \mathrm{E}_2) \cup a) = r_\mathrm{N}((\mathrm{Y}_0 - a) \cap \mathrm{E}_2)$. Disto, temos

$$\begin{aligned}\eta(\mathrm{Y}_0) &= r_1(\mathrm{Y}_0 \cap \mathrm{E}_1) + r_2(\mathrm{Y}_0 \cap \mathrm{E}_2) - r_\mathrm{L}(\mathrm{Y}_0 \cap \mathrm{T}) \\ &= r_1((\mathrm{Y}_0 - a) \cap \mathrm{E}_1) + 1 + r_2((\mathrm{Y}_0 - a) \cap \mathrm{E}_2) - r_\mathrm{L}((\mathrm{Y}_0 - a) \cap \mathrm{T}) - 1 \\ &= r_1((\mathrm{Y}_0 - a) \cap \mathrm{E}_1) + r_2((\mathrm{Y}_0 - a) \cap \mathrm{E}_2) - r_\mathrm{L}((\mathrm{Y}_0 - a) \cap \mathrm{T}) \\ &= \eta(\mathrm{Y}_0 - a),\end{aligned}$$

o que contradiz $\eta(\mathrm{Y}_0) < \eta(\mathrm{Y}_0 - a)$. Argumento análogo para o caso em que $a \in \mathrm{cl}_1((\mathrm{Y}_0 - a) \cap \mathrm{E}_1)$ e $a \notin \mathrm{cl}_2((\mathrm{Y}_0 - a) \cap \mathrm{E}_2)$. ⊣

Podemos escrever

$$\begin{aligned}\mathrm{Y}_0 \cap \mathrm{E}_1 &= (\mathrm{X} - \mathrm{E}_2) \cup (\mathrm{Y}_0 \cap \mathrm{T}) \\ \mathrm{Y}_0 \cap \mathrm{E}_2 &= (\mathrm{X} - \mathrm{E}_1) \cup (\mathrm{Y}_0 \cap \mathrm{T}),\end{aligned}$$

de modo que tais uniões sejam disjuntas. De $\mathrm{Y}_0 \cap \mathrm{E}_1 \notin \mathcal{I}_1$ e $\mathrm{Y}_0 \cap \mathrm{E}_2 \notin \mathcal{I}_2$, vemos que:

$$\begin{aligned}r_1(\mathrm{Y}_0 \cap \mathrm{E}_1) &< |(\mathrm{X} - \mathrm{E}_2) \cup (\mathrm{Y}_0 \cap \mathrm{T})| \\ &= r_1(\mathrm{X} - \mathrm{E}_2) + r_\mathrm{L}(\mathrm{Y}_0 \cap \mathrm{T}) \\ r_2(\mathrm{Y}_0 \cap \mathrm{E}_2) &< |(\mathrm{X} - \mathrm{E}_1) \cup (\mathrm{Y}_0 \cap \mathrm{T})| \\ &= r_2(\mathrm{X} - \mathrm{E}_1) + r_\mathrm{L}(\mathrm{Y}_0 \cap \mathrm{T}).\end{aligned}$$

Vamos analisar dois casos:

(1) Suponhamos que $r_\mathrm{L}(\mathrm{Y}_0 \cap \mathrm{T}) = 2$. Sabemos que $\mathrm{Y}_0 \subseteq \mathrm{cl}_\mathrm{U}(\mathrm{X})$, e assim, $\mathrm{T} \subseteq \mathrm{cl}_\mathrm{U}(\mathrm{X})$. Se existe $b \in \mathrm{T}$ tal que $b \notin \mathrm{cl}_1(\mathrm{X} \cap \mathrm{E}_1)$, então $r_1((\mathrm{X} \cap \mathrm{E}_1) \cup b) = r_1(\mathrm{X} \cap \mathrm{E}_1) + 1$. Nesse caso, vemos que $b \in \mathrm{cl}_2(\mathrm{X} \cap \mathrm{E}_2)$, e assim, $r_\mathrm{U}(\mathrm{X}) = r_\mathrm{U}(\mathrm{X} \cup b) = r_\mathrm{U}(\mathrm{X}) + 1$, o que é uma contradição. Isto mostra que $\mathrm{T} \subseteq \mathrm{cl}_1(\mathrm{X} \cap \mathrm{E}_1) \cap \mathrm{cl}_\mathrm{N}(\mathrm{X} \cap \mathrm{E}_2)$. Neste caso valem os itens (2.1) e (2.2) do enunciado.

(2) Suponhamos que $r_\mathrm{L}(\mathrm{Y}_0 \cap \mathrm{T}) = 1$. Existe $a \in \mathrm{T}$ tal que $\mathrm{Y}_0 \cap \mathrm{T} = \{ a \}$. Nesse caso, temos $\mathrm{Y}_0 \cap \mathrm{E}_1 = (\mathrm{X} - \mathrm{E}_2) \cup a$ e $\mathrm{Y}_0 \cap \mathrm{E}_2 = (\mathrm{X} - \mathrm{E}_1) \cup a$. Como $\mathrm{Y}_0 \cap \mathrm{E}_1 \notin \mathcal{I}_1$ e $\mathrm{Y}_0 \cap \mathrm{E}_2 \notin \mathcal{I}_2$, segue que $a \in \mathrm{cl}_1(\mathrm{X} - \mathrm{E}_2) \cap \mathrm{cl}_2(\mathrm{X} - \mathrm{E}_1)$. ⊣

II.5 MATROIDES DE GANHO E DE VIÉS

Apresentaremos nesta seção a noção de matroide de ganho. O Teorema II.5.12 garante que estas matroides são linearmente representáveis e os Teoremas II.5.14 e II.5.15 apresentam condições suficientes para que amálgamas próprias de certas classes de matroides de ganho sejam linearmente representáveis. As referências principais desta seção são D. Mayhew, M. Newman e G. Whittle [12] e T. Zaslavsky [24].

Suponhamos que G seja um grafo. Uma orientação de uma aresta $e \in \mathrm{E}(\mathrm{G})$ que incide aos vértices u, $v \in \mathrm{V}(\mathrm{G})$ é um elemento do conjunto $\{ (u, v), (v, u) \}$. Um *grafo orientado* é um par $(\mathrm{G}, \Delta_\mathrm{G})$, no qual $\Delta_\mathrm{G} : \mathrm{E}(\mathrm{G}) \longrightarrow \mathrm{V}(\mathrm{G})^2$ é uma função que mapeia cada aresta de G a uma de suas orientações. A função Δ_G é chamada de *orientação* de G. Dada uma orientação Δ_G de um grafo G, denotamos por Δ_G^-

a *orientação oposta* de Δ_G, que é obtida pela reversão de todas as orientações das arestas diferentes de loops. Podemos identificar a função Δ_G com o conjunto das triplas (e, u, v), nos quais $e \in E(G)$ e $\Delta_G(e) = (u, v)$. Fazendo o mesmo para Δ_G^-, vemos que $(e, u, v) \in \Delta_G^-$ sse $(e, v, u) \in \Delta_G$. Suponhamos que (G, Δ_G) seja um grafo orientado e que $(\Gamma, \cdot, 1)$ seja um grupo multiplicativo. Se $\varphi : \Delta_G \longrightarrow \Gamma$ é uma função, então podemos estendê-la para uma função $\Phi : \Delta_G \cup \Delta_G^- \longrightarrow \Gamma$ chamada *função de ganho de* G, que é definida pondo:

$$\Phi(e, u, v)^{n} = \begin{cases} \varphi(e, u, v), & \text{se } (e, u, v) \in \Delta_G \text{ e} \\ \varphi(e, v, u)^{-1}, & \text{se } (e, u, v) \in \Delta_G^- - \Delta_G. \end{cases}$$

Um *grafo de ganho* é um par (G, Φ) no qual (G, Δ_G) é um grafo orientado e Φ é uma função de ganho de G. Se e é uma aresta que incide aos vértices u e v, então dizemos que $\Phi(e, u, v) \in \Gamma$ é o *ganho* da aresta e no grafo de ganho. O ganho de uma aresta é dito unitário quando é igual a $1 \in \Gamma$. Dado um (v_1, v_m)-passeio $W = v_1, e_1, v_2, \ldots, v_m, e_m, v_{m+1}$ de G, podemos definir o ganho de W pondo

$$\Phi(W) = \Phi(e_1, v_1, v_2) \cdots \Phi(e_m, v_m, v_{m+1}).$$

Um *percurso* de um ciclo C do grafo G é um passeio fechado de C que não repete arestas de C. Uma *permutação cíclica* W_σ de um percurso $W = v_1, e_1, v_2, \ldots, v_m, e_m, v_1$ de C é um percurso

$$W_\sigma = v_{\sigma(1)}, e_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(m)}, e_{\sigma(m)}, v_{\sigma(1)},$$

onde $\sigma \in D_m$ é um elemento do grupo diedral D_m, que é isomorfo ao grupo das simetrias de polígonos regulares de m lados. Dado um percurso W de C, dizemos que $\Phi(W)$ é o *ganho de* C *segundo* W e dizemos que tal ganho é unitário quando $\Phi(W) = 1$. A seguinte proposição, cuja prova é elementar, relaciona permutações cíclicas de percursos com conjugação de ganhos.

PROPOSIÇÃO II.5.1. Suponhamos que C seja um ciclo de G de m arestas. Dado um percurso W de C se $\sigma \in D_m$ é um m-ciclo, então existe $g \in \Gamma$ tal que $\Phi(W_\sigma) = g \cdot \Phi(W) \cdot g^{-1}$.

Suponhamos que C seja um ciclo de G de m arestas. O *percurso oposto* de um percurso $W = v_1, e_1, v_2, \ldots, v_m, e_m, v_1$ de C é o percurso $W^{-1} = v_1, e_m, v_m, \ldots, v_2, e_1, v_1$. A construção do percurso oposto permite concluir que $\Phi(W) \cdot \Phi(W^{-1}) = 1$, e disto, obtemos o Lema II.5.2 a seguir:

LEMA II.5.2. Dados dois percursos W e W′ de um ciclo C de um grafo G, o ganho $\Phi(W')$ é conjugado ao ganho $\Phi(W)$ ou ao ganho $\Phi(W^{-1})$.

O Lema II.5.2 está de acordo com a ideia intuitiva de que em um ciclo com pelo menos três vértices existem essencialmente apenas dois sentidos para percorrê-lo. O que foi desenvolvido até aqui permite obter o seguinte teorema diretamente:

TEOREMA II.5.3 (Ganho Unitário). Suponhamos que G seja um grafo com pelo menos um ciclo. Dado um ciclo C de G, existe um percurso W de C tal que $\Phi(W) = 1$ sse $\Phi(W') = 1$ para todo percurso W′ de C.

[n] Se a aresta é um loop, então analisamos apenas a primeira cláusula da definição de Φ.

Relembremos do Exemplo II.1.1 que o conjunto de arestas de um ciclo de um grafo é chamado de circuito deste grafo. Denotemos por $\mathcal{C}(G)$ a coleção de todos os circuitos de um grafo G. Uma *coleção linear* de circuitos de G é uma coleção $\mathcal{L}(G) \subseteq \mathcal{C}(G)$ que satisfaz o seguinte: se $X, Y \in \mathcal{L}(G)$ são tais que $G \mid X \cup Y$ é um grafo theta, então $X \triangle Y \in \mathcal{L}(G)$[o]. Dizemos que um circuito é *equilibrado* quando pertence a $\mathcal{L}(G)$ e que é *desequilibrado* caso contrário. Um *grafo de viés* é uma lista $(G, \mathcal{L}(G))$, na qual G é um grafo e $\mathcal{L}(G)$ é uma coleção linear de circuitos de G.

EXEMPLO II.5.4 (Grafos de viés). Suponhamos que G seja um grafo e que $F \subseteq E(G)$ seja um conjunto não-vazio de arestas de G. Consideremos $\mathcal{L}(G)$ a coleção dos circuitos de G que tem interseção de tamanho par com F. Dados $X, Y \in \mathcal{L}(G)$, suponhamos que $G \mid X \cup Y$ seja um grafo theta. Independentemente da paridade do número de arestas de F em $X \cap Y$, vemos que $X \triangle Y$ tem um número par de arestas de F, e portanto, $X \triangle Y \in \mathcal{L}(G)$. ⊣

Dados um grafo de ganho (G, Φ) e um de seus ciclos C, se $\Phi(W) = 1$ para todo percurso W de C, então dizemos que E(C) é um circuito de G de *ganho unitário*. Denotemos por $\mathcal{L}(\Phi)$ a coleção de tais circuitos de G. O Corolário II.5.5 mostra que podemos formar um grafo de viés utilizando a coleção $\mathcal{L}(\Phi)$ de um grafo de ganho.

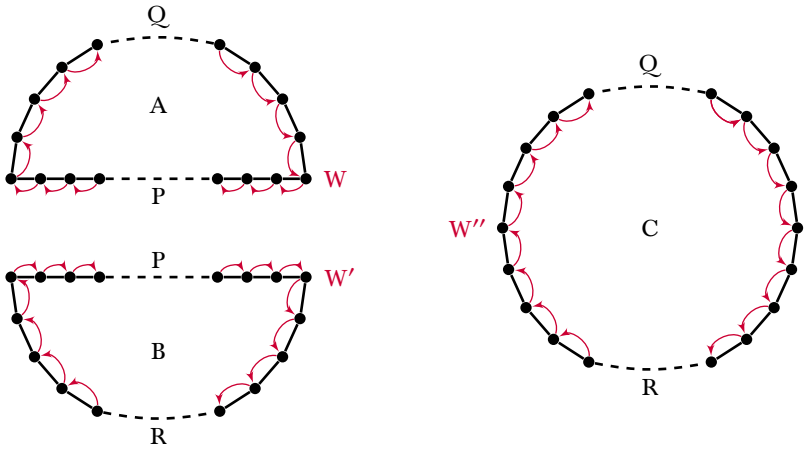

Figura II.5.1: Ilustração da ideia da demonstração do Corolário II.5.5. Se $G \mid X \cup Y$ é um grafo theta, então podemos percorrer os ciclos A e B tais que $E(A) = X$ e $E(B) = Y$, como mostram os grafos do lado esquerdo. Como os circuitos X e Y são equilibrados, indicamos um novo percurso para B sem perda de equilíbrio do circuito Y. Com o novo percurso, obtemos um percurso para C com $E(C) = X \triangle Y$, como mostra o grafo do lado direito. Por fim, basta observar que $X \triangle Y$ também é equilibrado.

COROLÁRIO II.5.5. [23, Proposição 5.1] A coleção $\mathcal{L}(\Phi)$ é linear. Disto segue que todo grafo de ganho (G, Φ) dá origem a um grafo de viés $(G, \mathcal{L}(\Phi))$.

Demonstração. Dados um ciclo C, um caminho $P \sqsubseteq C$ e um percurso W de C, denotemos por $\Phi_P(W)$ o ganho de P induzido por W. Tomemos $X, Y \in \mathcal{L}(\Phi)$ quaisquer, suponhamos que $G \mid X \cup Y$ seja um gafo theta e que A, B e C sejam os ciclos de G tais que $E(A) = X$, $E(B) = Y$ e $E(C) = X \triangle Y$. Observemos que $X \cap Y$ é não-vazio. Denotemos por P, Q e R os caminhos de G tais que $E(P) = X \cap Y$,

[o] $X \triangle Y = (X - Y) \cup (Y - X)$.

$E(Q) = X - Y$ e $E(R) = Y - X$. Tomemos os percursos W e W' de A e B, respectivamente, de modo que $\Phi_P(W) = \Phi_P(W')^{-1}$. Dado um percurso W'' de C tal que $\Phi_Q(W'') = \Phi_Q(W)$ e $\Phi_R(W'') = \Phi_R(W')$, segue que $\Phi(W'') = 1$. Do Teorema II.5.3, vemos que $X \triangle Y \in \mathcal{L}(\Phi)$. ⊣

Uma *pseudo-árvore* é um grafo e conexo com no máximo um ciclo e uma *pseudo-floresta* é um grafo cujas componentes conexas são todas pseudo-árvores. A Figura II.5.2 ilustra uma pseudo-árvore. Suponhamos que $(G, \mathcal{L}(G))$ seja um grafo de viés. Uma *pseudofloresta desequilibrada* de $(G, \mathcal{L}(G))$ é um pseudofloresta de G que não possui circuitos equilibrados. Definamos a coleção $\mathcal{I}_{\mathcal{L}}(G)$ dos subconjuntos $X \subseteq E(G)$ tais que $G \mid X$ são pseudoflorestas desequilibradas de $(G, \mathcal{L}(G))$.

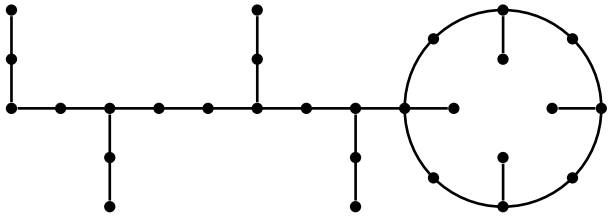

Figura II.5.2: Ilustração de uma pseudo-árvore.

Se H é um subgrafo de G que não é uma pseudofloresta desequilibrada, então H contém um ciclo equilibrado ou uma componente conexa com mais de um ciclo. Um grafo algema é desequilibrado quando seus dois circuitos são desequilibrados. Um grafo theta é desequilibrado quando seus três circuitos são desequilibrados. Denotemos por $\mathcal{C}_{\mathcal{L}}(G)$ a coleção dos subconjuntos $X \subseteq E(G)$ tais $X \in \mathcal{L}(G)$ ou $G \mid X$ é um grafo theta ou algema desequilibrados. Observemos que $\mathcal{C}_{\mathcal{L}}(G)$ é uma anticadeia.

LEMA II.5.6. [24, Teorema 2.1(e)] Se $X, Y \in \mathcal{C}_{\mathcal{L}}(G)$ são distintos e existe $a \in X \cap Y$, então existe $Z \in \mathcal{C}_{\mathcal{L}}(G)$ tal que $Z \subseteq (X \cup Y) - a$.

O lema anterior (cuja demonstração é enfadonha) foi provado por Zaslavsky [24] e será útil para obter o resultado do Teorema II.5.7. Da definição da coleção $\mathcal{I}_{\mathcal{L}}(G)$, do Lema II.5.6 e do Teorema II.2.6, segue:

TEOREMA II.5.7 (Matroide de Viés). [24, Teorema 2.1(c)] A coleção $\mathcal{I}_{\mathcal{L}}(G)$ é a coleção dos conjuntos independentes de uma matroide $M_{\mathcal{L}}(G)$ sobre $E(G)$ chamada de *matroide de viés*.

COROLÁRIO II.5.8. [15, Exercício 13(ii) sec. 12.2] Se $\mathcal{L}(G) = \mathcal{C}(G)$, então $M_{\mathcal{L}}(G) = M(G)$.

Demonstração. Neste caso, vemos que $I \in \mathcal{I}_{\mathcal{L}}(G)$ sse $I \subseteq E(G)$ não contém circuitos de G. O resultado segue então do Exemplo II.2.8. ⊣

Dizemos que $(H, \mathcal{L}(H))$ é um *subgrafo de viés* de $(G, \mathcal{L}(G))$ quando $H \sqsubseteq G$ e $\mathcal{L}(H) = \mathcal{L}(G) \cap 2^{E(H)}$.

COROLÁRIO II.5.9. Se $(H, \mathcal{L}(H))$ é um subgrafo de viés de $(G, \mathcal{L}(G))$, então $M_{\mathcal{L}}(G) \mid E(M_{\mathcal{L}}(H)) = M_{\mathcal{L}}(H)$.

Demonstração. Por definição, temos $H \sqsubseteq G$ e $\mathcal{L}(H) = \mathcal{L}(G) \cap 2^{E(H)}$. Dado $I \in \mathcal{I}_{\mathcal{L}}(H)$, sabemos que $H \mid I$ é uma pseudofloresta desequilibrada. Disto, segue que $G \mid I$ é uma pseudofloresta desequilibrada. Isto mostra que $I \in \mathcal{I}_{\mathcal{L}}(G)$. ⊣

Do Corolário II.5.5, sabemos que todo grafo de ganho (G, Φ) dá origem a um grafo de viés $(G, \mathcal{L}(\Phi))$, no qual $\mathcal{L}(\Phi)$ é a coleção dos circuitos de G de ganho unitário. Do Teorema II.5.7, obtemos então uma matroide de viés partindo do grafo de ganho (G, Φ). Tal matroide será chamada de ***matroide de ganho*** e a denotaremos por $M(\Phi) = (E(G), \mathcal{I}(\Phi))$.

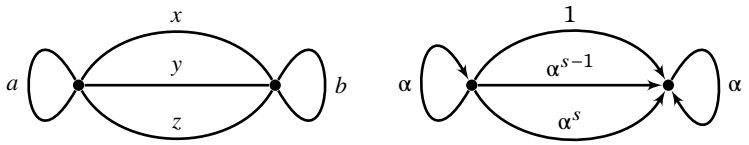

Figura II.5.3: Grafo do Exemplo II.5.10. Do lado esquerdo, apresentamos os rótulos das arestas e do lado direito, os seus ganhos.

EXEMPLO II.5.10 (Matroide de Ganho). Suponhamos que G seja o grafo da Figura II.5.3. Dado $s \in \mathbb{N}$ com $3 \leq s$, tomemos F um corpo e $\alpha \in F^{\times}$ com $s < \text{ord}(\alpha)$, onde $\text{ord}(\alpha)$ denota a ordem de α no grupo $F^{\times}$. Consideremos o grafo de ganho (G, Φ) obtido de G apresentado na mesma Figura II.5.3. Podemos formar a matroide $M(\Phi)$. Tomemos $X \subseteq E(G)$. Se $|X| \leq 2$, então $G \mid X$ é uma pseudofloresta desequilibrada. Se $3 \leq |X|$, então $G \mid X$ possui um grafo theta desequilibrado ou um grafo algema desequilibrado. Isso mostra que $I \in \mathcal{I}(\Phi)$ sse $|I| \leq 2$. Do Exemplo II.2.1, vemos que $M(\Phi) \cong U_{2,5}$. ⊣

Suponhamos que F seja um corpo, que G seja um grafo, que Δ_G seja uma orientação das arestas de G e que (G, Φ) seja um grafo de ganho obtido de G e de uma função de ganho $\Phi : \Delta_G \cup \Delta_G^- \longrightarrow F^{\times}$. Vamos supor ao longo do restante da seção que os contradomínios das funções de ganho são grupos multiplicativos de corpos. A ***matriz de incidência*** de (G, Φ) é a $V(G) \times E(G)$-matriz D_Φ dada por:

$$D_\Phi(u, e)^{\text{p}} = \begin{cases} 1, & \text{se } e \text{ não é um loop e } \Delta_G(e) = (u, -), \\ -\Phi(e, \Delta_G(e)), & \text{se } e \text{ não é um loop e } \Delta_G(e) = (-, u), \\ 1 - \Phi(e, \Delta_G(e)), & \text{se } e \text{ é um loop desequilibrado em } u, \\ 0, & \text{demais casos.} \end{cases}$$

Vamos mostrar que se (G, Φ) é um grafo de ganho e o contradomínio de Φ é o grupo multiplicativo de um corpo F, então a matroide de ganho $M(\Phi)$ é F-linearmente representável. Mais ainda, vamos mostrar que uma matriz representante de $M(\Phi)$ é D_Φ. Precisamos provar alguns resultados intermediários para alcançar tal objetivo.

LEMA II.5.11. [25, Teorema 2.1(a)] Suponhamos que (G, Φ) seja um grafo de ganho e que o contradomínio de Φ seja o grupo multiplicativo de um corpo F. Tomemos $X \subseteq E(G)$. Valem os seguintes resultados:

[p] Na primeira e na segunda cláusulas, os símbolos $\Delta_G(e) = (u, -)$ e $\Delta_G(e) = (-, u)$ denotam que u é a origem e o destino da aresta e segundo a orientação Δ_G, respectivamente.

(1) Se G | X é um ciclo, então $X \in \mathcal{L}(\Phi)$ sse as colunas correspondentes às arestas de X em D_Φ são linearmente dependentes.

(2) Se G | X é um grafo theta ou um grafo algema, então as colunas correspondentes às arestas de X em D_Φ são linearmente dependentes.

(3) Se G | X é uma floresta, então as colunas correspondentes às arestas de X em D_Φ são linearmente independentes.

(4) Se G | X é uma pseudofloresta que contém um ciclo, então as colunas correspondentes às arestas de X em D_Φ são linearmente independentes sse o único ciclo de G | X é desequilibrado.

Demonstração.

(1) Podemos supor que C = G | X é um ciclo com pelo menos três vértices. Enumeremos os elementos de X na forma $e_1, \ldots, e_m$ e denotemos por $\Phi_1, \ldots, \Phi_m$ seus ganhos respectivos de modo que $\Phi(C) = \Phi_1 \cdots \Phi_m$. Obtemos então a submatriz

$$D = \begin{bmatrix} 1 & & & & & -\Phi_m \\ -\Phi_1 & 1 & & & & \\ & -\Phi_2 & 1 & & & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & -\Phi_{m-1} & 1 \end{bmatrix}$$

da matriz D_Φ de modo que as colunas de D correspondam às arestas de C e as linhas correspondam aos vértices na ordem do percurso que segue por $e_1, \ldots, e_m$, nesta ordem. Os elementos omitidos em D são todos nulos. Os demais elementos das colunas que correspondem às arestas de C em D_Φ que não são elementos de D são todos nulos. Observemos que $\det(D) = 1 - \Phi(C)$. Do Teorema II.5.3, segue o resultado.

(2) Em virtude do primeiro item, podemos supor que todos os ciclos de H = G | X são desequilibrados. Suponhamos que $m = |X|$ e $n = |V(H)|$. Temos $n < m$. Do Teorema do Núcleo e da Imagem, vemos que as colunas de D_Φ correspondentes às arestas de H são linearmente dependentes.

(3) Cada folha corresponde a uma única entrada não-nula na respectiva linha da submatriz induzida pelas arestas da árvore. O resultado segue por indução desse argumento.

(4) Do primeiro item, sabemos que se o ciclo é equilibrado, então as colunas correspondentes às arestas de X em D_Φ são linearmente dependentes. Suponhamos que o único ciclo de H = G | X seja desequilibrado e que seu ganho seja $\Phi(C)$. Sabemos que $|V(H)| = |E(H)|$. Consideremos D a submatriz obtida de D_Φ tomando apenas as colunas correspondentes às arestas de H. Cada coluna possui apenas duas entradas não-nulas. Podemos supor que a orientação de G foi escolhida de modo que o bloco correspondente ao ciclo C na matriz D seja da forma da matriz apresentada no primeiro item. Ao escalonarmos a matriz D, vamos obter uma diagonal principal que tem uma entrada da forma $1 - \Phi(C)$ e todas as demais iguais à 1. Como C é desequilibrado, vemos que $1 - \Phi(C) \neq 0$. Disto, segue que as colunas de D são linearmente independentes. ⊣

TEOREMA II.5.12 (Representabilidade da Matroide de Ganho). Se (G, Φ) é um grafo de ganho, então $M(\Phi) = M(D_\Phi)$.

Demonstração. Segue do Lema II.5.11 que $I \in \mathcal{I}(\Phi)$ sse as colunas correspondentes aos elementos de I em D_Φ são linearmente independentes sse os rótulos das colunas são independentes em $M(D_\Phi)$. ⊣

Suponhamos que F seja um corpo, que $s \in \mathbb{N}$ seja tal que $3 \leq s$ e que $\alpha \in F^\times$ seja tal que $s < \mathrm{ord}(\alpha)$. Consideremos o grafo de ganho $\Gamma(F, s, \alpha)$ da Figura II.5.4 [12]. Denotamos por $M_\Gamma(s, \alpha)$ a matroide de ganho obtida deste grafo.

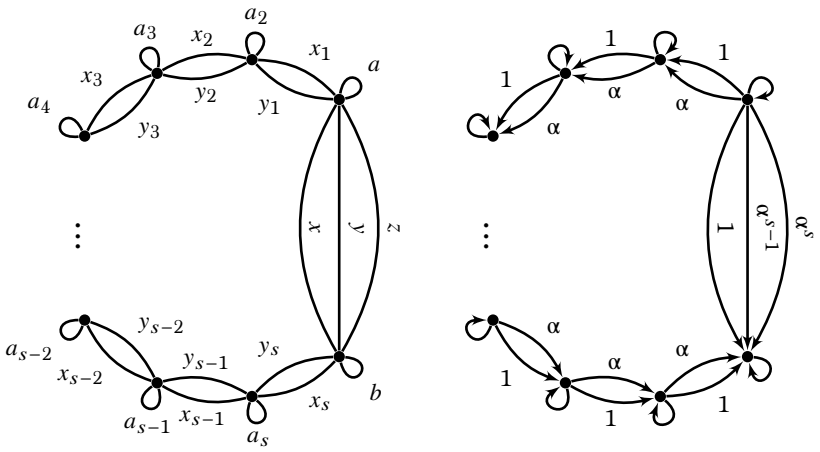

Figura II.5.4: A figura apresenta o grafo de ganho $\Gamma(F, s, \alpha)$ usado na construção da matroide de ganho $M_\Gamma(s, \alpha)$. Do lado esquerdo, apresentamos os rótulos das arestas e do lado direito, os seus ganhos. Os ganhos dos loops são α e foram omitidos na figura para facilitar a leitura. Os rótulos dos vértices são $u_1, \ldots, u_{s+1}$. As arestas x_i, y_i incidem aos vértices u_i e u_{i+1} para cada $i \in \{1, \ldots, s\}$. O grafo $\Gamma(F, s, \alpha)$ tem $s + 1$ vértices e $3s + 4$ arestas.

Do mesmo modo, suponhamos que $t \in \mathbb{N}$ seja tal que $3 \leq t$ e que $\beta \in F^\times$ seja tal que $2t(t-1) < \mathrm{ord}(\beta)$. Consideremos o grafo de ganho $\Delta(F, t, \beta)$ da Figura II.5.5 [12]. Denotamos por $M_\Delta(t, \beta)$ a matroide de ganho obtida deste grafo. A partir deste ponto, vamos denotar por $L \cong U_{2,5}$ a matroide do Exemplo II.5.10. Escrevamos T = E(L). Do Corolário II.5.9, vemos que $M_\Gamma(s, \alpha) \mid T = L$ e $M_\Delta(s, \beta) \mid T = L$. Suponhamos que F seja um corpo, que $3 \leq s$ seja um número inteiro e que $\alpha \in F^\times$ seja tal que $2s(s-1) < \mathrm{ord}(\alpha)$. Do Teorema II.4.9, segue que existe a amálgama própria $M_\Gamma(s, \alpha) \oplus_L M_\Delta(s, \alpha)$. Os seguintes resultados dizem respeito à representabilidade linear de amálgamas deste tipo.

LEMA II.5.13. Suponhamos que F seja um corpo, que $s \in \mathbb{N}$ seja tal que $3 \leq s$, que $\alpha \in F^\times$ seja tal que $2s(s-1) < \mathrm{ord}(\alpha)$ e que (G, Φ) seja o grafo de ganho da Figura II.5.6. A matroide M(Φ) é uma amálgama de $M_\Gamma(s, \alpha)$ e $M_\Delta(s, \alpha)$.

Demonstração. Os grafos de ganho $\Gamma(F, s, \alpha)$ e $\Delta(F, s, \alpha)$ são subgrafos de ganho de (G, Φ). Do Corolário II.5.9, segue que M(Φ) é uma amálgama de $M_\Gamma(s, \alpha)$ e $M_\Delta(s, \alpha)$. ⊣

O Teorema II.5.14 a seguir mostra sob quais condições amálgamas próprias das matroides obtidas dos grafos de ganho das Figuras II.5.4 e II.5.5 são linearmente representáveis.

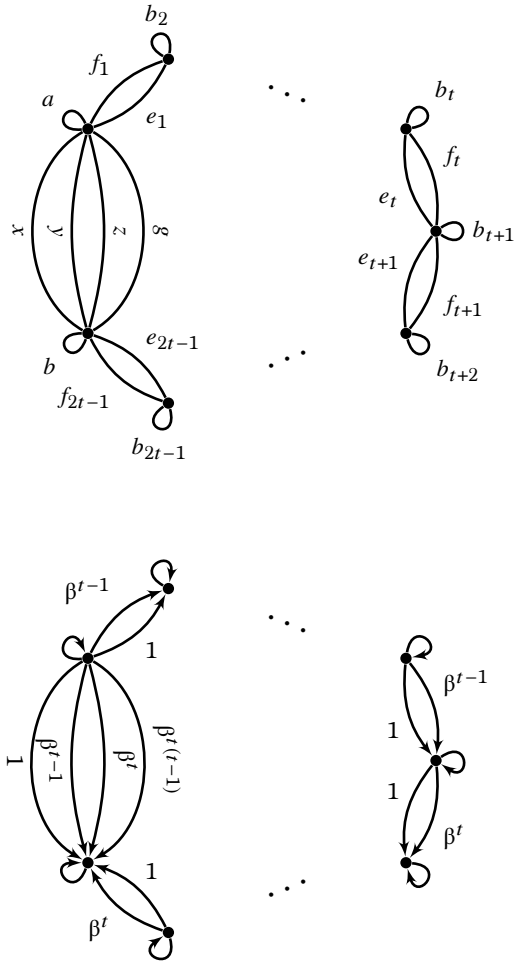

Figura II.5.5: A figura apresenta o grafo de ganho $\Delta(\mathrm{F}, t, \beta)$ usado na construção da matroide de ganho $\mathrm{M}_\Delta(t, \beta)$. Acima, apresentamos os rótulos das arestas e abaixo, os seus ganhos. Os ganhos dos loops são β e foram omitidos na figura para facilitar a leitura. Os rótulos dos vértices são $v_1, \ldots, v_{2t}$. As arestas e_i e f_i incidem aos vértices v_i e v_{i+1} para cada $i \in [2t-1]$. O grafo $\Delta(\mathrm{F}, t, \beta)$ tem $2t$ vértices e $6t+2$ arestas.

TEOREMA II.5.14 (Amálgama Própria Representável). [12, Lema 5.2] Suponhamos que F seja um corpo, que $3 \leq s$ seja um número inteiro e que $\alpha \in \mathrm{F}^{\times}$ seja tal que $2s(s-1) < \mathrm{ord}(\alpha)$. A matroide $\mathrm{M}_{\Gamma}(s,\alpha) \oplus_{\mathrm{L}} \mathrm{M}_{\Delta}(s,\alpha)$ é linearmente F-representável.

Demonstração. Suponhamos que (G,Φ) seja o grafo de ganho da Figura II.5.6. Do Lema II.5.13 e da definição de amálgama livre, segue que todo conjunto independente em $\mathrm{M}(\Phi)$ é independente em $\mathrm{M}_{\Gamma}(s,\alpha) \oplus_{\mathrm{L}} \mathrm{M}_{\Delta}(s,\alpha)$. Basta mostrar que todo conjunto dependente em $\mathrm{M}(\Phi)$ é dependente em $\mathrm{M}_{\Gamma}(s,\alpha) \oplus_{\mathrm{L}} \mathrm{M}_{\Delta}(s,\alpha)$. Escrevamos $\mathrm{M}_1 = \mathrm{M}_{\Gamma}(s,\alpha)$ e $\mathrm{M}_2 = \mathrm{M}_{\Delta}(s,\alpha)$. Suponhamos que $\mathrm{C} \in \mathcal{C}(\mathrm{M}(\Phi))$. Disto, vemos que $\mathrm{C} \in \mathcal{L}(\Phi)$ ou $\mathrm{G} \mid \mathrm{C}$ é um grafo theta ou algema desequilibrados. Podemos assumir que $\mathrm{C} \not\subseteq \mathrm{E}_1$ e $\mathrm{C} \not\subseteq \mathrm{E}_2$. Para fixar uma notação, denotemos por w o vértice com loop a e por w' o vértice com loop b. Consideremos também $u_2, \ldots, u_s$ os vértices com loops $a_2, \ldots, a_s$ e $v_2, \ldots, v_{2s-1}$ os vértices com loops $b_2, \ldots, b_{2s-1}$. Escrevamos $\mathrm{E} = \mathrm{E}_1 \cup \mathrm{E}_2$ e $\mathrm{T} = \mathrm{E}(\mathrm{L})$.

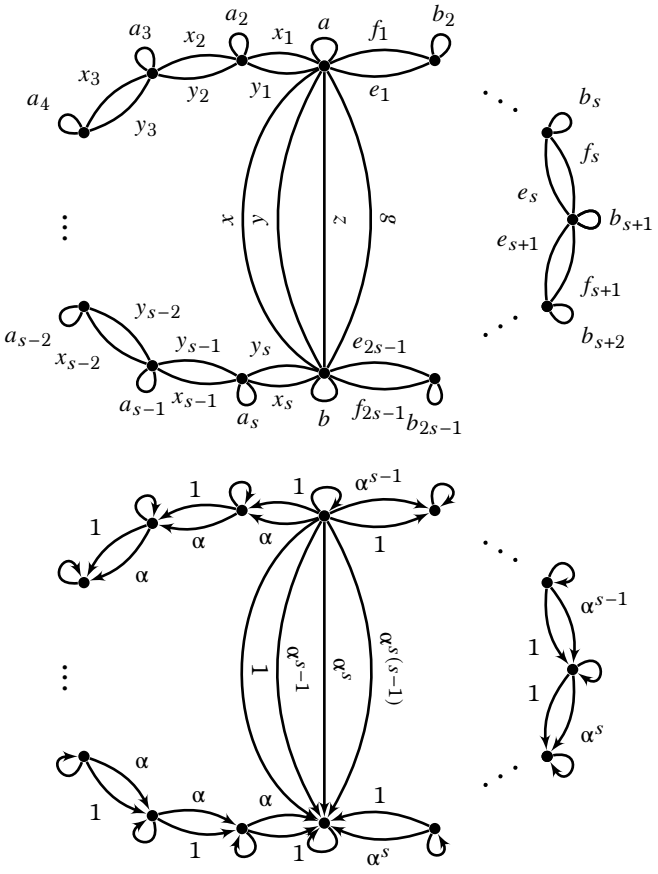

Figura II.5.6: Grafo de ganho (G,Φ) do Lema II.5.13 e do Teorema II.5.14. Acima, apresentamos os rótulos das arestas e abaixo, os seus ganhos. Do Corolário II.5.9, sabemos que $\mathrm{M}_{\Gamma}(s,\alpha)$ e $\mathrm{M}_{\Delta}(s,\alpha)$ são restrições de $\mathrm{M}(\Phi)$. O grafo (G,Φ) tem $3s-1$ vértices e $9s+1$ arestas.

(1) No primeiro caso, vamos supor que $\mathrm{C} \in \mathcal{L}(\Phi)$.

Afirmação 1. Não existe $e \in C$ que incide a w e w'.

Demonstração. Suponhamos que C possua uma aresta que incide a w e w'. Neste caso, segue de $C \not\subseteq E_1$ e $C \not\subseteq E_2$ que tal aresta é g e que $G \mid C$ contém um caminho cuja sequência de vértices é $w, u_2, \ldots, u_s, w'$. As arestas deste caminho são elementos de $E - E_2$, e portanto, o produto dos ganhos das arestas deste caminho é α^j com $j \leq s$. Como $G \mid C$ é um ciclo e seu ganho é unitário, vemos que $\alpha^j = \alpha^{s(s-1)}$. Da hipótese de que $3 \leq s$ e $2s(s-1) < \mathrm{ord}(\alpha)$, segue que $s < s(s-1)$. Disto, obtemos $0 < s(s-1) - j < \mathrm{ord}(\alpha)$ com $\alpha^{s(s-1)-j} = 1$, o que é uma contradição. ⊣

Da Afirmação 1, vemos que $G \mid C$ é um ciclo Hamiltoniano, i.e. um ciclo tal que $V(G \mid C) = V(G)$. Suponhamos que α^j seja o produto dos ganhos das arestas de um caminho em $G \mid C$ cuja sequência de vértices é $w, u_2, \ldots, u_s, w'$. Sabemos que $0 \leq j \leq s$. Suponhamos que $\alpha^{p(s-1)+qs}$ seja o produto dos ganhos das arestas de um caminho em $G \mid C$ cuja sequência de vértices é $w, v_2, \ldots, v_{2s-1}, w'$. Sabemos que $0 \leq p \leq s$ e $0 \leq q \leq s-1$, e assim, $0 \leq p(s-1) + qs \leq 2s(s-1)$. Disto, vemos que $\alpha^j = \alpha^{p(s-1)+qs}$. Da hipótese de que $3 \leq s$ e $2s(s-1) < \mathrm{ord}(\alpha)$ e da suposição $\Phi(C) = 1$, obtemos $j = p(s-1) + qs$. Das restrições de j, p e q, vemos que $j \in \{0, s-1, s\}$.

(1.1) Se $j = 0$, então as arestas do caminho em $G \mid C$ cuja sequência de vértices é $w, u_2, \ldots, u_s, w'$ são $x_1, \ldots, x_s$. Para $p(s-1)+qs = 0$ devemos ter $p = q = 0$. Disto, segue que as arestas do caminho em $G \mid C$ cuja sequência de vértices é $w, v_2, \ldots, v_{2s-1}, w'$ são $e_1, \ldots, e_{2s-1}$. Neste caso, obtemos $x \in \mathrm{cl}_1(C - E_2) \cap \mathrm{cl}_2(C - E_1)$ com $x \in T$.

(1.2) Se $j = s - 1$, então podemos supor (sem perda de generalidade) que as arestas do caminho em $G \mid C$ cuja sequência de vértices é $w, u_2, \ldots, u_s, w'$ são $x_1, y_2 \ldots, y_s$. Para $p(s-1) + qs = s - 1$ devemos ter $p = 1$ e $q = 0$. Podemos supor então (sem perda de generalidade) que as arestas do caminho em $G \mid C$ cuja sequência de vértices é $w, v_2, \ldots, v_{2s-1}, w'$ são $f_1, e_2 \ldots, e_{2s-1}$. Neste caso, obtemos $y \in \mathrm{cl}_1(C - E_2) \cap \mathrm{cl}_2(C - E_1)$ com $y \in T$.

(1.3) Se $j = s$, então as arestas do caminho em $G \mid C$ cuja sequência de vértices é $w, u_2, \ldots, u_s, w'$ são $y_1, \ldots, y_s$. Para $p(s-1) + qs = s$ devemos ter $p = 0$ e $q = 1$. Podemos supor (sem perda de generalidade) que as arestas do caminho em $G \mid C$ cuja sequência de vértices é $w, v_2, \ldots, v_{2s-1}, w'$ são $e_1, \ldots, e_s, f_{s+1}, e_{s+2}, \ldots, e_{2s-1}$. Neste caso, obtemos $z \in \mathrm{cl}_1(C - E_2) \cap \mathrm{cl}_2(C - E_1)$ com $z \in T$.

Em todos os casos anteriores, vemos que existe um elemento de T que pertence ao conjunto $\mathrm{cl}_1(C-E_2) \cap \mathrm{cl}_2(C-E_1)$. Segue do Teorema II.4.13 que C é dependente em $M_1 \oplus_L M_2$.

(2) Suponhamos que $G \mid C$ seja um grafo theta ou algema desequilibrados. Segue de $C \not\subseteq E_1$ e $C \not\subseteq E_2$ que existe em C uma aresta de $E_1 - E_2$ e uma aresta de $E_2 - E_1$. Vamos analisar dois casos:

(2.1) Tomemos $\{i, j\} = \{1, 2\}$. Suponhamos que $G \mid C - E_i$ seja um caminho que conecta w a w'. Todo vértice de $G \mid C - E_i$ tem grau no máximo dois em $G \mid C - E_i$. Disto, vemos que quando $G \mid C$ é um grafo algema desequilibrado os dois ciclos desequilibrados de $G \mid C$ estão em $G \mid C \cap E_i$. Vemos também que

quando $G \mid C$ é um grafo theta desequilibrado, temos um ciclo desequilibrado de $G \mid C$ em $G \mid C \cap E_i$. Não existe um caminho em $G \mid C \cap E_i$ que conecta os ciclos desequilibrados caso estes ciclos sejam distintos, já que circuitos são minimais e valem $C \not\subseteq E_1$ e $C \not\subseteq E_2$. Isso mostra que $G \mid C \cap E_i$ contém um caminho que conecta um ciclo desequilibrado ao vértice w e contém um caminho que conecta um ciclo desequilibrado ao vértice w' e estes caminhos não compartilham arestas. Uma ilustração do que foi discutido é apresentada na Figura II.5.7.

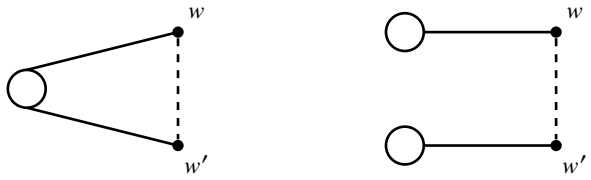

Figura II.5.7: A figura apresenta o caso 2.1 da demonstração do Teorema II.5.14, no qual vemos que existem circuitos desequilibrados ligados aos vértices w e w' por caminhos em $G \mid C \cap E_i - T$. A linha tracejada corresponde ao caminho $G \mid C - E_i$.

Segue, portanto, que $a, b \in \mathrm{cl}_i(C \cap E_i)$, e assim, $T \subseteq \mathrm{cl}_i(C \cap E_i)$. Mais ainda, $G \mid (C - E_i) \cup (a \cup b)$ é um grafo algema desequilibrado, e portanto, $(C - E_i) \cup (a \cup b)$ é um circuito de M_j que gera T. Neste caso, obtemos $r_j((C - E_i) \cup T) = r_j(C - E_i) < r_j(C - E_i) + 2$. Do Teorema II.4.13, segue que C é dependente em $M_1 \oplus_L M_2$.

(2.2) Suponhamos que $G \mid C - E_1$ e $G \mid C - E_2$ não sejam caminhos que conectam w a w'. Se $G \mid C - E_1$ é uma floresta, então segue de $G \mid C$ não ter vértices de grau um que $G \mid C - E_1$ é um caminho que conecta w a w', o que é uma contradição. Disto, segue que $G \mid C - E_1$ e $G \mid C - E_2$ possuem ciclos desequilibrados. Da conexidade de $G \mid C$, segue que w ou w' é vértice de um caminho que conecta o ciclo de $G \mid C - E_1$ ao ciclo de $G \mid C - E_2$. Suponhamos que w satisfaça essa condição. Neste caso, vemos que $G \mid (C - E_2) \cup a$ é um grafo algema desequilibrado, e portanto, $a \in \mathrm{cl}_1(C - E_2)$. Vemos também que $G \mid (C - E_1) \cup a$ é um grafo algema desequilibrado, e portanto, $a \in \mathrm{cl}_2(C - E_1)$. Disto, vemos que $a \in T$ é tal que $a \in \mathrm{cl}_1(C - E_2) \cap \mathrm{cl}_2(C - E_1)$. Do Teorema II.4.13, segue que C é dependente em $M_1 \oplus_L M_2$.

Da Proposição II.2.7, concluímos que $M(\Phi) = M_\Gamma(s, \alpha) \oplus_L M_\Delta(s, \alpha)$ e do Teorema II.5.12, segue que $M_\Gamma(s, \alpha) \oplus_L M_\Delta(s, \alpha)$ é linearmente F-representável. ⊣

O Teorema II.5.15 a seguir mostra sob quais condições amálgamas próprias das matroides obtidas dos grafos de ganho das Figuras II.5.4 e II.5.5 não são linearmente representáveis.

TEOREMA II.5.15 (Amálgama Própria Não-Representável). [12, Lema 5.3] Suponhamos que F seja um corpo, que $3 \leq s, t$ sejam números inteiros distintos e que $\alpha \in F^\times$ seja tal que $\max\{ s, 2t(t-1) \} < \mathrm{ord}(\alpha)$. A matroide $M_\Gamma(s, \alpha) \oplus_L M_\Delta(t, \alpha)$ não é linearmente representável.

Demonstração. O conjunto dos loops desequilibrados de $\Gamma(F, s, \alpha)$ é $B_\Gamma = \{ a_2, \ldots, a_s, a, b \}$ e o conjunto dos loops desequilibrados de $\Delta(F, t, \alpha)$ é $B_\Delta = \{ b_2, \ldots, b_{2t-1}, a, b \}$. Definamos $B = B_\Gamma \cup B_\Delta$. O grafo $\Gamma(F, s, \alpha)$ dá origem à matroide $M_1 = M_\Gamma(s, \alpha)$ e o grafo $\Delta(F, t, \alpha)$ dá origem à matroide $M_2 = M_\Delta(t, \alpha)$. Do

Teorema II.4.9, segue que existe a matroide $U = M_1 \oplus_L M_2$. As seguintes afirmações serão úteis para mostrar que B é uma base de U. Escrevamos $E = E_1 \cup E_2$ e $T = E_1 \cap E_2$.

Afirmação 1. Valem $r_1((B - E_2) \cup T) = r_1(B - E_2) + 2$ e $r_2((B - E_1) \cup T) = r_2(B - E_1) + 2$.

Demonstração. Sabemos que $B - E_2 \subseteq B_\Gamma$, e assim, $r_1(B - E_2) = |B_\Gamma| - 2$. Por outro lado, $r_1(B_\Gamma) = |B_\Gamma|$. Sabemos que $B - E_2 = B_\Gamma - T$, e portanto, $r_1((B - E_2) \cup T) = r_1(B_\Gamma)$. Disto, obtemos $r_1(B - E_2) = r_1((B - E_2) \cup T) - 2$, e portanto, $r_1((B - E_2) \cup T) = r_1(B - E_2) + 2$. Raciocínio análogo para a outra igualdade. ⊣

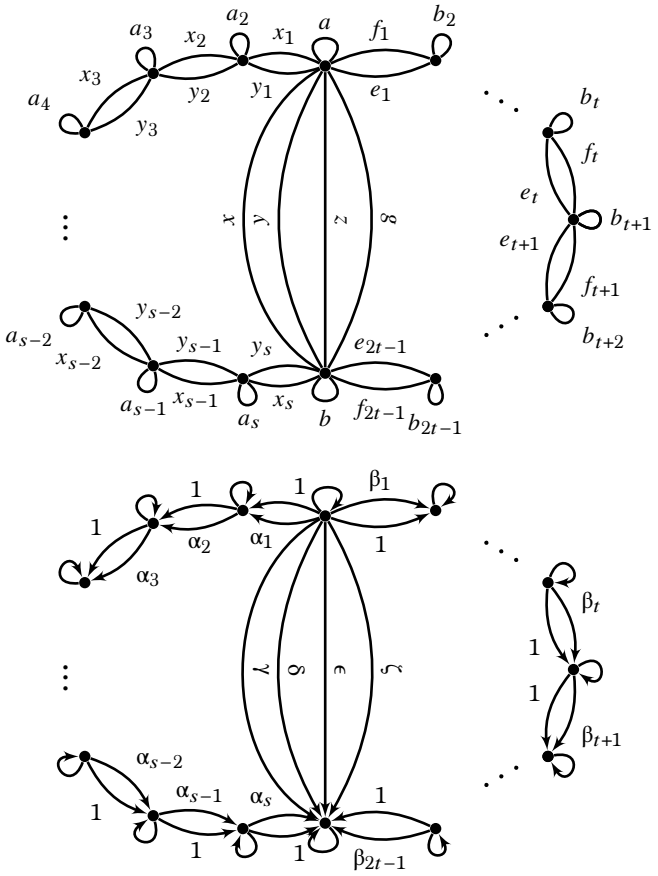

Figura II.5.8: A figura apresenta o grafo de ganho hipotético (G, Φ) da Afirmação 4 obtido pela análise dos circuitos fundamentais da matroide $M_\Gamma(s, \alpha) \oplus_L M_\Delta(t, \alpha)$ relativos à base B formada por todos os loops. Acima, apresentamos os rótulos das arestas e abaixo, os seus ganhos.

Afirmação 2. Para todo $e \in T$, temos $e \notin \mathrm{cl}_1(B - E_2) \cap \mathrm{cl}_2(B - E_1)$.

Demonstração. Basta observar que nenhuma aresta de T dá origem a um circuito quando unida a $B - E_1$. A mesma observação vale para $B - E_2$. ⊣

Suponhamos que U seja linearmente K-representável e que D seja uma matriz que a representa sobre o corpo K. Das Afirmações 1 e 2 e do Teorema II.4.13, segue que $B \in \mathcal{I}(U)$. Dado $e \in E - B$, existe único $C \in \mathcal{C}_1$ ou único $C \in \mathcal{C}_2$ tal que $e \in C$ e $C \subseteq B \cup e$. Estes circuitos tem três elementos cada. Isto mostra que B é um conjunto $\subseteq$-maximal em $\mathcal{I}(U)$, e assim, B é uma base de U. Como os loops dos grafos que dão origem às matroides M_1 e M_2 não são equilibrados, podemos assumir que o bloco correspondente aos elementos de B em D é da forma λI_r, onde $r = |B|$ e $\lambda \in K^\times$. Podemos escrever

$$D = \begin{bmatrix} \lambda I_r & A \end{bmatrix},$$

onde cada coluna de A tem a primeira entrada não-nula igual a $1 \in K$.

Afirmação 3. A matriz D é a matriz de incidência de um grafo de ganho.

Demonstração. Basta observar que:

(1) Se $e \in B$, então a coluna de D correspondente à aresta e possui uma única entrada não-nula.

(2) Suponhamos que c seja uma coluna de A. Existe $e \in E$ correspondente à coluna c. Como todo circuito fundamental de U relativo à base B tem tamanho três, segue que existem e', $e'' \in B$ tais que $\{e, e', e''\}$ é um circuito (fundamental) de U. Se c' e c'' são as colunas de λI_r correspondentes às arestas e' e e'', respectivamente, então existem escalares r, s, $t \in K$ nem todos nulos tais que $rc + sc' + tc'' = 0$. Disto vemos que c tem exatamente duas entradas não-nulas. ⊣

Da Afirmação 3, vemos que a matriz D é uma matriz de incidência de um grafo de ganho (G, Φ), onde o ganho toma valores em $K^\times$. Vemos também que $U \cong M(\Phi)$.

Afirmação 4. O grafo de ganho (G, Φ) é como aquele da Figura II.5.8.

Demonstração. Este resultado é obtido analisando os circuitos fundamentais relativos à base B e a matriz D:

(1) Para cada elemento de B, obtemos um vértice. Podemos definir w como sendo o vértice com loop a e w' como sendo o vértice com loop b. Os demais vértices são $u_2, \ldots, u_s$ para os loops $a_2, \ldots, a_s$ e $v_2, \ldots, v_{2t-1}$ para os loops $b_2, \ldots, b_{2t-1}$.

(2) As arestas x, y, z e g formam circuitos fundamentais com os loops a e b, e portanto, x, y, z e g incidem aos vértices w e w'.

(3) As arestas x_1 e y_1 formam circuitos fundamentais com os loops a e a_2, e portanto, x_1 e y_1 incidem aos vértices w e u_2. As arestas x_s e y_s formam circuitos fundamentais com os loops a_s e b, e portanto, x_s e y_s incidem aos vértices u_s e w'.

(4) As arestas e_1 e f_1 formam circuitos fundamentais com os loops a e b_2, e portanto, e_1 e f_1 incidem aos vértices w e v_2. As arestas e_{2t-1} e f_{2t-1} formam circuitos fundamentais com os loops b_{2t-1} e b, e portanto, e_{2t-1} e f_{2t-1} incidem aos vértices v_{2t-1} e w'.

(5) Para as demais arestas as incidências coincidem com as incidências dos grafos que dão origem às matroides M_1 e M_2. ⊣

Nos dirigimos para o fim da demonstração do teorema. Vamos, a partir deste ponto, analisar os ganhos das arestas do grafo obtido na Afirmação 4 utilizando a sua matriz de incidência D obtida na Afirmação 3. Escalonando as linhas de D (se necessário) podemos supor que:

$$\Phi(x_1, w, u_2) = \Phi(x_s, u_s, w') = \Phi(e_1, w, v_2) = 1.$$

Definamos:

$$\begin{array}{llll} \Phi(y_1, w, u_2) & = \alpha_1 & \Phi(y_s, u_s, w') = \alpha_s & \Phi(f_1, w, v_2) = \beta_1 \\ \Phi(f_{2t-1}, v_{2t-1}, w') & = \beta_{2t-1} & \Phi(x, w, w') = \gamma & \Phi(y, w, w') = \delta \\ \Phi(z, w, w') & = \epsilon & \Phi(g, w, w') = \zeta. & \end{array}$$

Vamos usar o fato de que $U \cong M(\Phi)$ para decidir propriedades das arestas de (G, Φ) partindo do que já sabemos sobre estas arestas em $\Gamma(F, s, \alpha)$ e $\Delta(F, t, \alpha)$.

(1) Sabemos que $\{ x_1, \ldots, x_s, x \}$ é um circuito equilibrado em $\Gamma(F, s, \alpha)$ e que $\{ e_1, \ldots, e_{2t-1}, x \}$ é um circuito equilibrado em $\Delta(F, t, \alpha)$, e portanto, sabemos que $\{ x_1, \ldots, x_s, x \}$ é um circuito de M_1 e $\{ e_1, \ldots, e_{2t-1}, x \}$ é um circuito de M_2. Do Teorema II.4.13 e da eliminação de x, segue que o conjunto $\{ x_1, \ldots, x_s, e_1, \ldots, e_{2t-1} \}$ é um circuito equilibrado em (G, Φ). Podemos assumir que $\Phi(x_i, u_i, u_{i+1}) = 1$ para cada $2 \leq i \leq 2s-1$ e que $\Phi(e_i, v_i, v_{i+1}) = 1$ para cada $2 \leq i \leq 2t-2$. Disto, temos $\Phi(e_{2t-1}, v_{2t-1}, w') = 1$.

(2) Sabemos que $\{ x_1, \ldots, x_s, x \}$ é um circuito equilibrado de $\Gamma(F, s, \alpha)$, e portanto, tal conjunto é um circuito de M_1. Disto, segue que $\{ x_1, \ldots, x_s, x \}$ também é um circuito equilibrado em (G, Φ), e assim, $\gamma = 1$. Escrevamos $\Phi(y_i, u_i, u_{i+1}) = \alpha_i$ para cada $2 \leq i \leq s-1$.

(2.1) Para cada $1 \leq i \leq s$, vemos que $(\{ y_1, \ldots, y_s \} - y_i) \cup \{ x_i, y \}$ é um circuito equilibrado de $\Gamma(F, s, \alpha)$, e portanto, de (G, Φ). O produto dos ganhos dessas arestas em (G, Φ) é $\alpha_1 \cdots \alpha_s \alpha_i^{-1} \delta^{-1} = 1$, e portanto, $\alpha_i = \alpha_1 \cdots \alpha_s \delta^{-1}$. Isto mostra que $\alpha_1 = \cdots = \alpha_s$. Fazendo $\alpha_0 = \alpha_1 \cdots \alpha_s \delta^{-1}$, obtemos $\alpha_i = \alpha_0$ para cada $1 \leq i \leq s$ e também $\delta = \alpha_0^{s-1}$.

(2.2) O conjunto $\{ y_1, \ldots, y_s, z \}$ é um circuito equilibrado de $\Gamma(F, s, \alpha)$, e portanto, de (G, Φ). O produto dos ganhos dessas arestas em (G, Φ) é $\alpha_0^s \epsilon^{-1} = 1$, e portanto, $\epsilon = \alpha_0^s$.

(3) Escrevamos $\Phi(f_i, v_i, v_{i+1}) = \beta_i$ para cada $2 \leq i \leq s-1$. Para cada $1 \leq i \leq t$, vemos que $(\{ e_1, \ldots, e_{2t-1} \} - e_i) \cup \{ f_i, y \}$ é um circuito equilibrado de $\Delta(F, t, \alpha)$, e portanto, de (G, Φ). O produto dos ganhos dessas arestas em (G, Φ) é $\beta_i \delta^{-1} = 1$, e assim, $\beta_i = \alpha_0^{s-1}$ para cada $1 \leq i \leq t$. Para cada $t+1 \leq i \leq 2t-1$, vemos que $(\{ e_1, \ldots, e_{2t-1} \} - e_i) \cup \{ f_i, z \}$ é um circuito equilibrado de $\Delta(F, t, \alpha)$, e portanto, de (G, Φ). O produto dos ganhos dessas arestas em (G, Φ) é $\beta_i \epsilon^{-1} = 1$, e portanto, $\beta_i = \alpha_0^s$ para cada $t+1 \leq i \leq 2t-1$.

(4) Resta agora determinar o valor de ζ. Os conjuntos

$$\{ f_1, \ldots, f_t, e_{t+1}, \ldots, e_{2t-1}, g \}$$
$$\{ e_1, \ldots, e_t, f_{t+1}, \ldots, f_{2t-1}, g \}$$

são circuitos equilibrados de $\Delta(F, t, \alpha)$, e portanto, de (G, Φ). O produto dos ganhos do primeiro conjunto é $\alpha_0^{(s-1)t}\zeta^{-1} = 1$. O produto dos ganhos do segundo conjunto é $\alpha_0^{s(t-1)}\zeta^{-1} = 1$. Vemos, portanto, que $\alpha_0^s = \alpha_0^t$.

Tomemos $m = \text{ord}(\alpha_0)$ em $K^\times$. Como $s \neq t$, vemos que $m < \max\{s, t\}$. Se $m < s$, então $\{y_1, \ldots, y_m, x_{m+1}, \ldots, x_s, x\}$ é um circuito equilibrado de (G, Φ) e não é um circuito de U. Desta contradição, obtemos $m < t$. Neste caso, vemos que $\{f_1, \ldots, f_m, e_{m+1}, \ldots, e_{2t-1}, x\}$ é um circuito equilibrado de (G, Φ), já que o produto dos ganhos desse conjunto é $\alpha^{m(s-1)} = 1$. Por outro lado, tal conjunto não é um circuito de U. Desta contradição, vemos que $M_1 \oplus_L M_2$ não é linearmente representável. ⊣

Os Teoremas II.5.14 e II.5.15 que acabamos de provar são úteis para construir exemplos de amálgamas próprias com $L \cong U_{2,5}$. Um corolário importante destes teoremas é o seguinte:

COROLÁRIO II.5.16. A classe das matroides de ganho não é fechada pela construção de amálgamas.

Além do resultado do corolário anterior, observemos que o resultado do Teorema II.5.15 mostra que o conceito de independência abstrata estudado em Teoria de Matroides não coincide com a independência linear advinda de espaços vetoriais. Em outras palavras, a classe das matroides contém propriamente a classe das matroides linearmente representáveis.

III LINGUAGEM MS_0

III.1 SINTAXE E PROVA

Nesta seção serão apresentados resultados básicos sobre uma linguagem monádica de segunda ordem para Teoria de Matroides: a descrição sintática básica da linguagem lidará com regras de formação de palavras da linguagem e regras de dedução de teoremas na linguagem. Vamos apresentar uma linguagem baseada no que é feito por D. Mayhew, M. Newman e G. Whittle [12] com uma modificação para a adoção de uma notação prefixa como é feito por R. Shoenfield [17] para linguagens de primeira ordem.

Vimos no Capítulo II que a Teoria de Matroides estuda o conceito de independência abstrata que surge em diversas áreas da Matemática. Para que uma linguagem formal seja capaz de expressar sentenças significativas sobre matroides é necessário que possamos expressar que um conjunto é independente. Os itens a seguir descreverão o alfabeto Λ_{I} da linguagem monádica de segunda ordem $\mathrm{L_I}$ para Teoria de Matroides:

(1) Uma quantidade infinita e enumerável de *variáveis*

$$v_0, v_1, \ldots, v_m, \ldots$$

Tais símbolos serão usados para que possamos expressar sentenças que dizem respeito a conjuntos indivíduos. Utilizaremos os símbolos x, y e z como metavariáveis de símbolos de variáveis.

(2) Símbolos constantes:

(2.1) Uma quantidade finita de *constantes* de conjuntos de $\mathrm{L_I}$. Utilizaremos os símbolos c e k como metavariáveis de constantes. O papel desempenhado por constantes é o de dar nomes aos subconjuntos de elementos dos domínios das interpretações da linguagem e isto ficará claro na próxima seção.

(2.2) Uma quantidade finita de símbolos de *predicados* de $\mathrm{L_I}$. Utilizaremos Π^m como metavariável de um símbolo de predicado m-ádico qualquer. O símbolos de predicado usados na linguagem $\mathrm{L_I}$ são:

- Ind, que será usado para indicar se um conjunto é independente.
- Sng, que será usado para indicar se um conjunto é unitário.
- $\sqsubseteq$, que será usado para indicar se um conjunto é subconjunto de outro.

(2.3) Símbolos de conectivos lógicos de:

- Falsidade $\bot$.
- Conjunção $\wedge$.
- Disjunção $\vee$.
- Implicação $\rightarrow$.

Utilizaremos $\circ$ como metavariável dos conectivos $\wedge$ e $\vee$ e utilizaremos $\square$ como metavariável dos conectivos $\wedge$, $\vee$ e $\rightarrow$.

(2.4) Os seguintes símbolos de quantificadores:

- Quantificador existencial $\exists$.
- Quantificador universal $\forall$.

Utilizaremos Q como metavariável de um quantificador arbitrário e utilizaremos Q^* para o quantificador diferente de Q uma vez que Q for escolhido.

(3) Símbolos de parênteses esquerdo e direito, que são chamados de símbolos de pontuação. Os parênteses serão úteis para abreviações.

(4) Os símbolos de variáveis, conectivos, quantificadores, Sng e $\sqsubseteq$ são chamados de *símbolos lógicos* de L_I, enquanto os símbolos de constantes e Ind são chamados de *símbolos não-lógicos* de L_I.

(5) Diferentemente de outros textos, adotaremos uma notação prefixa para formação de fórmulas. Isto quer dizer que escreveremos $\wedge\varphi\psi$ no lugar da expressão mais comum $(\varphi \wedge \psi)$, por exemplo.

Uma *expressão* sobre o alfabeto Λ_I é qualquer sequência finita de elementos de Λ_I e o *fecho de Kleene* $\Lambda_I^\star$ deste alfabeto é o conjunto de todas as expressões sobre este alfabeto. Um *termo* de L_I é um símbolo de constante de conjunto ou de variável. Vamos utilizar a meta-expressão $r(t_1, \ldots, t_m)$ para indicar que os termos $t_1, \ldots, t_m$ ocorrem na expressão r quando for necessário. Vamos agora apresentar as regras de formação recursiva de fórmulas da linguagem L_I:

(1) Uma *fórmula atômica* de L_I é uma expressão da forma $\Pi^m t_1 \cdots t_m$, na qual Π^m é um símbolo de predicado m-ádico e $t_1, \ldots, t_m$ são termos. Uma *fórmula inicial* de L_I é ou uma fórmula atômica ou $\bot$.

(2) Uma *fórmula* da linguagem L_I é definida recursivamente da seguinte maneira:

(2.1) Toda fórmula inicial de L_I é uma fórmula de L_I.

(2.2) Se φ e ψ são fórmulas de L_I, então

$$\wedge\varphi\psi \qquad \vee\varphi\psi \qquad \rightarrow\varphi\psi$$

são fórmulas de L_I. Lemos estas fórmulas como "φ e ψ", "φ ou ψ" e "se φ, então ψ", respectivamente.

(2.3) Se φ é uma fórmula de L_I na qual ocorre a variável x e não ocorrem as expressões $\exists x$ ou $\forall x$, então

$$\exists x\varphi \qquad \forall x\varphi$$

são fórmulas de L_I. Lemos estas fórmulas como "existe x tal que φ" e "para todo x, φ", respectivamente. A fórmula φ é chamada de *escopo* dos quantificadores.

(2.4) Apenas são fórmulas da linguagem L_I as expressões sobre Λ_I obtidas por um número finito de aplicações das regras de formação apresentadas nos itens 2.1, 2.2 e 2.3.

Enquanto as expressões sobre o alfabeto Λ_I são sequências finitas quaisquer de símbolos deste alfabeto, as fórmulas de L_I são expressões especiais que permitirão representar sentenças relacionadas a Teoria de Matroides. Observemos que definimos os termos e as fórmulas de L_I seguindo uma notação prefixa, e portanto, os termos e as fórmulas são escritos na forma $su_1 \cdots u_m$, onde s é um símbolo de Λ_I e $u_1, \ldots, u_m$ são fórmulas ou termos de L_I em quantidade m chamada de *índice* de s. Os índices dos símbolos do alfabeto da linguagem são os seguintes:

(1) Os índices variáveis, constantes e de $\bot$ são 0.

(2) O índice de um predicado m-ádico é m.

(3) Os índices dos conectivos $\wedge$, $\vee$ e $\rightarrow$ e dos quantificadores $\exists$ e $\forall$ são 2.

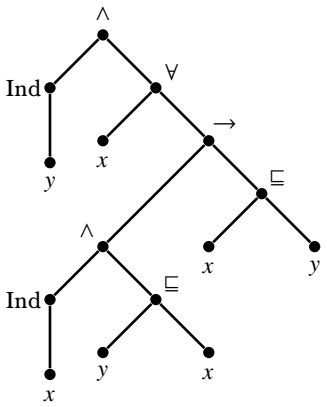

Figura III.1.1: Árvore sintática da fórmula analisada no Exemplo III.1.1. A árvore é ordenada da esquerda para a direita e de cima para baixo. Segundo esta ordenação, segue que nesta árvore o primeiro sucessor do vértice com rótulo $\forall$ é um vértice com rótulo x e o segundo sucessor do vértice com rótulo $\forall$ é o vértice com rótulo $\rightarrow$.

EXEMPLO III.1.1 (Fórmulas). A seguinte expressão[a] sobre Λ_{I} é uma fórmula de L_{I}:

$$\wedge\,\mathrm{Ind}\,y\forall x \rightarrow \wedge\,\mathrm{Ind}\,x \sqsubseteq yx \sqsubseteq xy.$$

A Figura III.1.1 apresenta uma árvore sintática que ajudará na visualização da análise do exemplo. A árvore é ordenada da esquerda para a direita e de cima para baixo. O primeiro símbolo $\wedge$ é um conectivo com índice dois, e portanto, ele deve ser seguido de duas fórmulas. As duas fórmulas são as fórmulas

$$\mathrm{Ind}\,y \quad \text{e} \quad \forall x \rightarrow \wedge\,\mathrm{Ind}\,x \sqsubseteq yx \sqsubseteq xy,$$

nesta ordem. A fórmula $\mathrm{Ind}\,a$ inicia com o símbolo de predicado monádico Ind e este é seguido pela variável y. A fórmula $\forall x \rightarrow \wedge\,\mathrm{Ind}\,x \sqsubseteq yx \sqsubseteq xy$ inicia com o quantificador universal $\forall$, que tem índice dois. O quantificador $\forall$ deve ser seguido de uma variável e de uma fórmula na qual ocorre esta variável, nesta ordem. Neste caso concreto, a variável é x e a fórmula é $\rightarrow \wedge\,\mathrm{Ind}\,x \sqsubseteq yx \sqsubseteq xy$. Tal fórmula inicia com o conectivo $\rightarrow$, que tem índice dois, e portanto, ele deve ser seguido de duas fórmulas. As duas fórmulas são

$$\wedge\,\mathrm{Ind}\,x \sqsubseteq yx \quad \text{e} \quad \sqsubseteq xy,$$

nesta ordem. A fórmula atômica $\sqsubseteq xy$ inicia com o símbolo de predicado diádico $\sqsubseteq$ e este é seguido dos termos x e y, nesta ordem. A fórmula $\wedge\,\mathrm{Ind}\,x \sqsubseteq yx$ inicia com o conectivo $\wedge$ de índice dois, e portanto, ele é seguido das fórmulas

$$\mathrm{Ind}\,x \quad \text{e} \quad \sqsubseteq yx,$$

nesta ordem. Analisamos estas duas fórmulas de maneiras análogas àquelas feitas anteriormente nas quais ocorrem os mesmos símbolos. ⊣

[a]Desejamos expressar com a fórmula deste exemplo, segundo as noções semânticas que serão apresentadas na próxima seção, que y é um conjunto independente $\subseteq$-maximal.

Seguindo o que é feito por J. Shoenfield [17], vamos usar a expressão *designadores* para designar termos e fórmulas da linguagem. Duas expressões r e s sobre Λ_{I} são *compatíveis* sse uma pode ser obtida da outra pela concatenação de uma expressão à direita. Por exemplo, as expressões $\wedge rs$ e $\wedge r$ são compatíveis, pois $\wedge rs$ é obtida de $\wedge r$ pela concatenação de s à direita de $\wedge r$. Observemos que se rs e tu são compatíveis, então r e t são compatíveis. Observemos também que se rs e rt são compatíveis, então s e t são compatíveis. Designadores são as expressões sobre o alfabeto Λ_{I} sintaticamente corretas segundo as regras de formação (de termos e fórmulas) e a moral do Lema III.1.2 a seguir é a seguinte: se obtivermos duas expressões $r_1 \cdots r_m$ e $s_1 \cdots s_m$ compatíveis ao concatenarmos designadores de maneira correta segundo as regras de formação apresentadas, então os designadores são os mesmos e ocorrem na mesma ordem.

LEMA III.1.2 (Propriedade de Legibilidade Única). [17, Lema 1] Se $r_1, \ldots, r_m$ e $s_1, \ldots, s_m$ são designadores tais que $r_1 \cdots r_m$ e $s_1 \cdots s_m$ são compatíveis, então $r_i = s_i$ para cada $i \in \{1, \ldots, m\}$.

Demonstração. A prova é feita por indução no comprimento da expressão $r_1 \cdots r_m$. Podemos escrever $r_1 = ur'_1 \cdots r'_i$, onde u é um símbolo de índice i. Da compatibilidade de $r_1 \cdots r_m$ e $s_1 \cdots s_m$, segue que r_1 e s_1 são compatíveis, e portanto, $s_1 = us'_1 \cdots s'_i$ (já que duas expressões que começam com símbolos distintos não podem ser compatíveis). Do passo de indução, segue que $r'_1 = s'_1$, ..., $r'_i = s'_i$, e assim, $r_1 = s_1$. Disto e da compatibilidade de $r_1 \cdots r_m$ e $s_1 \cdots s_m$, segue que $r_2 \cdots r_m$ e $s_2 \cdots s_m$ são compatíveis. Do passo de indução, segue que $r_2 = s_2$, ..., $r_m = s_m$. O resultado segue então do Princípio de Indução. ⊣

O seguinte teorema é consequência do Lema III.1.2 e pode ser provado por indução no comprimento das expressões. Tal resultado de unicidade de escrita é importante para garantir a unicidade das interpretações de fórmulas da linguagem objeto que segue da legibilidade única dos designadores.

TEOREMA III.1.3. [17, Teorema da Formação] Designadores são escritos unicamente da forma $su_1 \cdots u_m$, onde s é um símbolo de Λ_{I} e u_1, ..., u_m são designadores em quantidade m compatível com o índice de s.

O seguinte lema mostra que podemos determinar o início de um termo ou de uma fórmula observando nestas expressões as ocorrências dos símbolos do alfabeto Λ_{I}. Por exemplo, na fórmula do Exemplo III.1.1, podemos identificar o ínicio da fórmula $\rightarrow \wedge \mathrm{Ind}\, x \sqsubseteq yx \sqsubseteq xy$ observando a ocorrência do símbolo $\rightarrow$ de índice dois. E podemos identificar em $\rightarrow \wedge \mathrm{Ind}\, x \sqsubseteq yx \sqsubseteq xy$ o início da fórmula $\wedge \mathrm{Ind}\, x \sqsubseteq yx$ observando a ocorrência do símbolo $\wedge$ de índice dois. O resultado também é provado por indução no comprimento dos designadores.

LEMA III.1.4. [17, Lema 2] Toda ocorrência de um símbolo de Λ_{I} em um designador r inicia a ocorrência de um designador em r.

O seguinte teorema formaliza a noção de ocorrência de um designador em outro designador, e assim, poderemos dizer que uma fórmula ocorre em outra fórmula sem problemas. Por exemplo, a fórmula $\mathrm{Ind}\, x$ ocorre na fórmula do Exemplo III.1.1. O resultado também é provado por indução no comprimento dos designadores.

TEOREMA III.1.5. [17, Teorema da Ocorrência] Suponhamos que s seja um símbolo de Λ_{I} de índice m e que $r_1, \ldots, r_m$ sejam designadores. Se um designador r ocorre em $sr_1 \cdots r_m$, então ou $r = sr_1 \cdots r_m$ ou existe $i \in \{1, \ldots, m\}$ tal que r ocorre em r_i.

As *fórmulas livres de quantificadores* de $\mathrm{L_I}$ são as fórmulas de $\mathrm{L_I}$ nas quais não ocorrem símbolos de quantificadores. Uma ocorrência de uma variável x é *ligada* em uma fórmula φ se ela se dá em uma fórmula $\exists x \psi(x)$ que ocorre em φ. Caso contrário, dizemos que a ocorrência é *livre*. Dizemos que uma variável é livre (resp. ligada) em uma fórmula se alguma de suas ocorrências nesta fórmula é livre (resp. ligada). Por exemplo, a variável x é livre na fórmula $\mathrm{Ind}\, x$ e é ligada na fórmula $\forall x\, \mathrm{Ind}\, x$. Observemos que x é tanto livre quanto ligada na fórmula $\vee\, \mathrm{Ind}\, x \forall x\, \mathrm{Ind}\, x$. Abreviaremos $\sqsubseteq rs$ na forma $(r \sqsubseteq s)$ e abreviaremos $\square \psi \phi$ na forma $(\psi \square \phi)$. Por simplicidade, vamos usar o termo "fórmula" tanto para fórmulas, quanto para suas abreviações. Omitiremos a expressão "de $\mathrm{L_I}$" em frases cujo contexto linguístico formal é transparente.

EXEMPLO III.1.6 (Símbolos Definidos). No alfabeto de $\mathrm{L_I}$ não incluímos símbolos para negação $\neg$, verdade $\top$ ou equivalência material $\leftrightarrow$. Definimos $\top$, $\neg$ e $\leftrightarrow$ por meio das abreviações $\top$, $(\neg\varphi)$ e $(\psi \leftrightarrow \phi)$ das fórmulas $(\bot \to \bot)$, $(\varphi \to \bot)$ e $((\psi \to \phi) \wedge (\phi \to \psi))$, respectivamente. Omitiremos os parênteses inicial e final de uma abreviação caso não haja ambiguidade. Para evitar ainda mais o uso desnecessário de parênteses, vamos adotar também a seguinte convenção: $\neg$ tem precedência sobre $\wedge$ e $\vee$ e estes têm precedência sobre $\to$ e $\leftrightarrow$. Adotaremos também a associação à direita de um mesmo conectivo. Um exemplo concreto dessas convenções é a abreviação

$$\mathrm{Ind}\, y \wedge \forall x(\mathrm{Ind}\, x \wedge y \sqsubseteq x \to x \sqsubseteq y)^{\mathrm{b}}$$

da fórmula do Exemplo III.1.1. ⊣

Uma fórmula na qual não ocorrem variáveis livres é chamada de *sentença*. Estamos aptos para discutir substituição de variáveis em fórmulas e termos. Dados dois termos s e t e uma variável x, denotamos a *substituição de x por t em s* por $\frac{t}{x}s$ e a definimos recursivamente da seguinte maneira:

(1) Se x não ocorre em s, então $\frac{t}{x}s = s$.

(2) Se x ocorre em s, então segue do Teorema III.1.5 que $s = x$. Neste caso, definimos $\frac{t}{x}s = t$.

Dados um termo t, uma variável x e uma fórmula φ, denotamos a *substituição de x por t em* φ por $\frac{t}{x}\varphi$ e a definimos recursivamente da seguinte maneira:

(1) Se φ é uma fórmula inicial, então:

- Se $\varphi = \bot$, então $\frac{t}{x}\varphi = \bot$.
- Se $\varphi = \Pi^m t_1 \cdots t_m$, então $\frac{t}{x}\varphi = \Pi^m \frac{t}{x}t_1 \cdots \frac{t}{x}t_m$

(2) Se φ não é inicial, então:

- Se $\varphi = \square\alpha\beta$, então $\frac{t}{x}\varphi = \square\frac{t}{x}\alpha\frac{t}{x}\beta$.

[b] Em geral as pessoas acham essa forma mais fácil de ler quando comparada àquela do Exemplo III.1.1.

- Se $\varphi = Qx\alpha(x)$, então $\frac{t}{x}\varphi = \varphi$.
- Se $\varphi = Qy\alpha(y)$ e $y \neq x$, então $\frac{t}{x}\varphi = Qy\frac{t}{x}\alpha(y)$.

O processo pode ser generalizado para substituições simultâneas de várias variáveis por termos em termos e fórmulas, que denotaremos por $\frac{t_1,\ldots,t_m}{x_1,\ldots,x_m}s$ e $\frac{t_1,\ldots,t_m}{x_1,\ldots,x_m}\varphi$, respectivamente. Vamos seguir D. van Dalen [20] e J. Shoenfield [17] e exigir que as substituições sigam certos critérios bem-definidos. Substituições de variáveis por variáveis podem dar origem a ocorrências ligadas no escopo de um quantificador (vide Exemplo III.1.7), modificando assim o significado de uma fórmula. Suponhamos que t seja um termo, que x seja uma variável e que φ seja uma fórmula. O termo t *é livre para* x *em* φ sse as variáveis de t em $\frac{t}{x}\varphi$ não são ligadas por quantificadores nesta fórmula. Observemos que uma variável que não ocorre em uma fórmula sempre é livre para qualquer variável que ocorra nesta mesma fórmula. Vamos assumir ao longo do texto que toda substituição cumpre com os critérios apresentados, a menos que seja dito explicitamente o contrário.

EXEMPLO III.1.7 (Substituição). A variável x não é livre para a variável y na fórmula

$$\mathrm{Ind}\, y \wedge \forall x(\mathrm{Ind}\, x \wedge y \sqsubseteq x \rightarrow x \sqsubseteq y)$$

do Exemplo III.1.1. De fato, nesta fórmula ocorre a fórmula $\forall x(\mathrm{Ind}\, x \wedge y \sqsubseteq x \rightarrow x \sqsubseteq y)$ na qual ocorre livre a variável y. Ao substituirmos a variável y por x, mudaremos totalmente o sentido da fórmula. Por outro lado, se z não ocorre na fórmula, então a substituição da variável y pela variável z não é problemática. ⊣

Até agora, lidamos com regras de formação para construir as sentenças da linguagem $\mathrm{L_I}$. Outro conceito importante em lógica é aquele da dedução. Vamos apresentar um sistema de dedução baseado em J. von Plato e S. Negri [13]. Um *sequente* é uma expressão da forma $\Gamma \Rightarrow \Delta$, onde Γ e Δ são multiconjuntos finitos de fórmulas denominados *contextos* do sequente [13, 18]. Os contextos Γ e Δ são chamados de *antecedente* e *sucedente* do sequente, respectivamente. Uma variável ocorre livre em um sequente se ela ocorre livre em alguma fórmula de algum contexto. Uma *inferência* é uma das expressões das formas

$$\frac{\Gamma_1 \Rightarrow \Delta_1}{\Gamma \Rightarrow \Delta} \qquad \frac{\Gamma_1 \Rightarrow \Delta_1 \quad \Gamma_2 \Rightarrow \Delta_2}{\Gamma \Rightarrow \Delta}$$

nas quais $\Gamma_1 \Rightarrow \Delta_1$ e $\Gamma_2 \Rightarrow \Delta_2$ são chamados de *sequentes superiores* da inferência e $\Gamma \Rightarrow \Delta$ é chamado de *sequente inferior* da inferência. Intuitivamente, sequentes superiores são as premissas de uma inferência e o sequente inferior é a conclusão da inferência. Suponhamos que $\Gamma_1, \ldots, \Gamma_m$ sejam multiconjuntos finitos de fórmulas. Abreviaremos a união $\Gamma_1 \cup \cdots \cup \Gamma_m$ dos multiconjuntos por $\Gamma_1, \ldots, \Gamma_m$. Se φ é uma fórmula, omitiremos as chaves $\{\, \varphi \,\}$ na notação de sequente. Por exemplo, abreviamos $\Gamma_1 \cup \Gamma_2 \cup \{\, \varphi \,\} \Rightarrow \Delta$ na forma $\Gamma_1, \Gamma_2, \varphi \Rightarrow \Delta$. Apresentando uma intuição de lógica clássica, um sequente da forma $\alpha_1, \ldots, \alpha_m \Rightarrow \beta_1, \ldots, \beta_n$ significa "se $\alpha_1 \wedge \cdots \wedge \alpha_m$, então $\beta_1 \vee \ldots \vee \beta_n$" [18]. Em outras palavras, se todas as fórmulas $\alpha_1, \ldots, \alpha_m$ são verdadeiras, então alguma das fórmulas $\beta_1, \ldots, \beta_n$ é verdadeira. Nesta interpretação intuitiva de sequentes, temos o seguinte:

- Se m é positivo e $n = 0$, então $\alpha_1, \ldots, \alpha_m \Rightarrow$ significa que $\alpha_1 \wedge \cdots \wedge \alpha_m$ é uma contradição.

- Se $m = 0$ e n é positivo, então $\Rightarrow \beta_1, \ldots, \beta_n$ significa que $\beta_1 \vee \cdots \vee \beta_n$ é uma tautologia.
- Se $m = 0$ e $n = 0$, então $\Rightarrow$ significa uma contradição.

Desejamos apresentar uma noção de prova em um sistema formal clássico baseado em um cálculo de sequentes. Um *sequente inicial* é um sequente da forma $\varphi, \Gamma \Rightarrow \Delta, \varphi$, onde φ é uma fórmula inicial e Γ e Δ são contextos quaisquer. Segundo a noção intuitiva de sequente, um sequente inicial da forma $\varphi \Rightarrow \varphi$ significa "se φ, então φ". A introdução deste tipo de sequentes em provas formais será representada da seguinte forma:

$$\frac{}{\varphi, \Gamma \Rightarrow \Delta, \varphi}\ \mathrm{A}$$

O rótulo A indicará em uma prova que o sequente $\varphi, \Gamma \Rightarrow \Delta, \varphi$ é um sequente inicial. A regra não tem premissas: é sempre lícito concluir φ em um contexto da suposição de φ neste contexto. Além de introduzir sequentes iniciais em provas, desejamos também transformá-los por meio de regras de inferência que governem as constantes lógicas da linguagem. As *regras lógicas* de dedução de sequentes são regras que lidam com constantes lógicas da linguagem à direita e à esquerda do símbolo $\Rightarrow$ [13, 18]. Vamos usar os índices E e D nos rótulos que indicam as regras para explicitar de qual lado do símbolo $\Rightarrow$ a regra atua. As regras indicadas com E e D correspondem à eliminação e introdução de constantes lógicas, respectivamente, em um sentido que ficará claro quando as apresentarmos.

($\bot$) A regra que rege o símbolo $\bot$ é a regra $\bot_{\mathrm{E}}$ apresentada na forma:

$$\frac{}{\bot, \Gamma \Rightarrow \Delta}\ \bot_{\mathrm{E}}$$

Segundo a noção intuitiva de sequente, um sequente da forma $\bot \Rightarrow \beta$ significa "se $\bot$, então β". A regra não tem premissas: partindo um resultado falso em um contexto, concluímos qualquer resultado neste contexto.

($\wedge$) As regras que regem o símbolo $\wedge$ são as regras $\wedge_{\mathrm{E}}$ e $\wedge_{\mathrm{D}}$ apresentadas nas formas:

$$\frac{\psi, \phi, \Gamma \Rightarrow \Delta}{\psi \wedge \phi, \Gamma \Rightarrow \Delta}\ \wedge_{\mathrm{E}} \qquad \frac{\Gamma \Rightarrow \Delta, \psi \qquad \Gamma \Rightarrow \Delta, \phi}{\Gamma \Rightarrow \Delta, \psi \wedge \phi}\ \wedge_{\mathrm{D}}$$

- Analisemos a regra $\wedge_{\mathrm{E}}$. Nela, temos os sequentes superior $\psi, \phi, \Gamma \Rightarrow \Delta$ e inferior $\psi \wedge \phi, \Gamma \Rightarrow \Delta$. Ela corresponde à eliminação do símbolo $\wedge$ no seguinte sentido: se algo em Δ segue de $\psi \wedge \phi$ em um contexto Γ, então este algo já seguia de ψ e ϕ neste mesmo contexto.
- Analisemos agora a regra $\wedge_{\mathrm{D}}$. Nela, temos os sequentes superiores $\Gamma \Rightarrow \Delta, \psi$ e $\Gamma \Rightarrow \Delta, \phi$ e o sequente inferior $\Gamma \Rightarrow \Delta, \psi \wedge \phi$. Ela corresponde à introdução do símbolo $\wedge$ no seguinte sentido: se em um mesmo contexto obtemos tanto ψ quanto ϕ, então obtemos $\psi \wedge \phi$ neste mesmo contexto. Lendo a regra de baixo para cima, vemos como a derivação de $\psi \wedge \phi$ se reduz às derivações de ψ e ϕ, isto é, que $\psi \wedge \phi$ é derivável sempre que tanto ψ quanto ϕ o forem.

($\vee$) As regras que regem o símbolo $\vee$ são as regras $\vee_{\mathrm{E}}$ e $\vee_{\mathrm{D}}$ apresentadas nas formas:

$$\frac{\psi, \Gamma \Rightarrow \Delta \qquad \phi, \Gamma \Rightarrow \Delta}{\psi \vee \phi, \Gamma \Rightarrow \Delta}\ \vee_{\mathrm{E}} \qquad \frac{\Gamma \Rightarrow \Delta, \psi, \phi}{\Gamma \Rightarrow \Delta, \psi \vee \phi}\ \vee_{\mathrm{D}}$$

- Analisemos a regra $\vee_{\mathrm{E}}$. Nela, temos os sequentes superiores $\psi, \Gamma \Rightarrow \Delta$ e $\phi, \Gamma \Rightarrow \Delta$ e o sequente inferior $\psi \vee \phi, \Gamma \Rightarrow \Delta$. Ela corresponde à eliminação do símbolo $\vee$ no seguinte sentido: se algo em Δ segue de $\psi \vee \phi$ em um contexto Γ, então este algo já seguia de ψ ou já seguia de ϕ neste mesmo contexto.
- Analisemos agora a regra $\vee_{\mathrm{D}}$. Nela, temos os sequentes superior $\Gamma \Rightarrow \Delta, \psi, \phi$ e inferior $\Gamma \Rightarrow \Delta, \psi \vee \phi$. Ela corresponde à introdução do símbolo $\vee$ no seguinte sentido: se em um mesmo contexto obtemos ψ ou ϕ, então obtemos $\psi \vee \phi$ neste mesmo contexto. Lendo a regra de baixo para cima, vemos como a derivação de $\psi \vee \phi$ se reduz às derivações de ψ ou de ϕ, isto é, que $\psi \vee \phi$ é derivável sempre que o for algum dentre ψ ou ϕ.

($\rightarrow$) As regras que regem o símbolo $\rightarrow$ são as regras $\rightarrow_{\mathrm{E}}$ e $\rightarrow_{\mathrm{D}}$ apresentadas na forma:

$$\frac{\Gamma \Rightarrow \Delta, \psi \qquad \phi, \Gamma \Rightarrow \Delta}{\psi \rightarrow \phi, \Gamma \Rightarrow \Delta}\ \rightarrow_{\mathrm{E}} \qquad \frac{\psi, \Gamma \Rightarrow \Delta, \phi}{\Gamma \Rightarrow \Delta, \psi \rightarrow \phi}\ \rightarrow_{\mathrm{D}}$$

- Analisemos a regra $\rightarrow_{\mathrm{E}}$. Nela, temos os sequentes superiores $\Gamma \Rightarrow \Delta, \psi$ e $\phi, \Gamma \Rightarrow \Delta$ e o sequente inferior $\psi \rightarrow \phi, \Gamma \Rightarrow \Delta$. Ela corresponde à eliminação do símbolo $\rightarrow$ no seguinte sentido: se algo em Δ segue de $\psi \rightarrow \phi$ em um contexto Γ, então este algo já seguia de ϕ neste contexto ou ψ já seguia deste contexto.
- Analisemos agora a regra $\rightarrow_{\mathrm{D}}$. Nela, temos os sequentes superior $\psi, \Gamma \Rightarrow \Delta, \phi$ e inferior $\Gamma \Rightarrow \Delta, \psi \rightarrow \phi$. Ela corresponde à introdução do símbolo $\rightarrow$ no seguinte sentido: se em um contexto obtemos ϕ da suposição hipotética de ψ, então obtemos $\psi \rightarrow \phi$ neste mesmo contexto. Lendo a regra de baixo para cima, vemos como a derivação de $\psi \rightarrow \phi$ se reduz às derivações de ψ ou de ϕ, isto é, que ϕ é derivável sempre que ψ o for.

($\exists$) As regras que regem o símbolo $\exists$ são as regras $\exists^{\bullet}_{\mathrm{E}}$ e $\exists_{\mathrm{D}}$ apresentadas na forma:

$$\frac{\frac{y}{x}\varphi(x), \Gamma \Rightarrow \Delta}{\exists x \varphi(x), \Gamma \Rightarrow \Delta}\ \exists^{\bullet}_{\mathrm{E}} \qquad \frac{\Gamma \Rightarrow \Delta, \exists x \varphi(x), \frac{t}{x}\varphi(x)}{\Gamma \Rightarrow \Delta, \exists x \varphi(x)}\ \exists_{\mathrm{D}}$$

Na regra $\exists^{\bullet}_{\mathrm{E}}$ exigimos que a variável y não ocorra livre em $\exists x \varphi(x), \Gamma \Rightarrow \Delta$. Esta condição é chamada de *condição de autovariável* da inferência.

- Analisemos a regra $\exists^{\bullet}_{\mathrm{E}}$. Nela, temos os sequentes superior $\frac{y}{x}\varphi(x), \Gamma \Rightarrow \Delta$ e inferior $\exists x \varphi(x), \Gamma \Rightarrow \Delta$. Ela corresponde à eliminação do símbolo $\exists$ no seguinte sentido: se algo em Δ segue de $\exists x \varphi(x)$ em um contexto Γ, então este

algo já seguia de $\frac{y}{x}\varphi(x)$ neste contexto, dada alguma restrição a testemunha arbitrária y. A restrição sobre a variável y ficará clara quando discutirmos semântica.

- Analisemos agora a regra $\exists_{\mathrm{D}}$. Nela, temos os sequentes superior $\Gamma \Rightarrow \Delta, \exists x\varphi(x), \frac{t}{x}\varphi(x)\varphi(x)$ e inferior $\Gamma \Rightarrow \Delta, \exists x\varphi(x)$. Ela corresponde à introdução do símbolo $\exists$ no seguinte sentido: se em um contexto obtemos $\frac{t}{x}\varphi(x)$ para algum termo t, então obtemos $\exists x\varphi(x)$ neste mesmo contexto. Lendo a regra de baixo para cima, vemos como a derivação de $\exists x\varphi(x)$ se reduz às derivações de $\frac{t}{x}\varphi(x)$, isto é, que $\exists x\varphi(x)$ é derivável sempre que obtivermos uma testemunha t que certifique $\frac{t}{x}\varphi(x)$.

(∀) As regras que regem o símbolo $\forall$ são as regras $\forall_{\mathrm{E}}$ e $\forall^{\bullet}_{\mathrm{D}}$ apresentadas na forma:

$$\frac{\frac{t}{x}\varphi(x), \forall x\varphi(x), \Gamma \Rightarrow \Delta}{\forall x\varphi(x), \Gamma \Rightarrow \Delta}\ \forall_{\mathrm{E}} \qquad \frac{\Gamma \Rightarrow \Delta, \frac{y}{x}\varphi(x)}{\Gamma \Rightarrow \Delta, \forall x\varphi(x)}\ \forall^{\bullet}_{\mathrm{D}}$$

Na regra $\forall^{\bullet}_{\mathrm{D}}$ exigimos que a variável y não ocorra livre em $\Gamma \Rightarrow \Delta, \forall x\varphi(x)$. Esta condição é chamada de ***condição de autovariável*** da inferência.

- Analisemos a regra $\forall_{\mathrm{E}}$. Nela, temos os sequentes superior $\frac{t}{x}\varphi(x), \forall x\varphi(x), \Gamma \Rightarrow \Delta$ e inferior $\forall x\varphi(x), \Gamma \Rightarrow \Delta$. Ela corresponde à eliminação do símbolo $\forall$ no seguinte sentido: se algo em Δ segue de $\forall x\varphi(x)$ em um contexto Γ, então este algo já seguia de $\frac{t}{x}\phi(x)$ neste contexto, para algum termo arbitrário t.
- Analisemos agora a regra $\forall^{\bullet}_{\mathrm{D}}$. Nela, temos os sequentes superior $\Gamma \Rightarrow \Delta, \frac{y}{x}\varphi(x)$ e inferior $\Gamma \Rightarrow \Delta, \forall x\varphi(x)$. Ela corresponde à introdução do símbolo $\forall$ no seguinte sentido: se em um contexto obtemos $\frac{y}{x}\varphi(x)$ para uma variavel arbitrária y, então obtemos $\forall x\varphi(x)$ neste mesmo contexto, dada alguma restrição sobre y. A restrição sobre o termo t ficará clara quando discutirmos semântica. Lendo a regra de baixo para cima, vemos como a derivação de $\forall x\varphi(x)$ se reduz à derivação $\frac{y}{x}\varphi(x)$, isto é, que $\forall x\varphi(x)$ é derivável sempre derivarmos $\frac{y}{x}\varphi(x)$ com algum grau correto de generalidade.

Além das regras que regem símbolos lógicos, temos também regras estruturais que lidam com os contextos. As regras dizem respeito ao enfraquecimento, à contração e ao corte. Não há regras para permutação, uma vez que os contextos são multiconjuntos.

(1) As regras estruturais de enfraquecimento são

$$\frac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}\ \mathrm{W}_{\mathrm{E}} \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \varphi}\ \mathrm{W}_{\mathrm{D}}$$

As regras de enfraquecimento permitem que ampliemos nosso estoque de fórmulas em um contexto.

(2) As regras estruturais de contração são

$$\frac{\varphi, \varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}\ \mathrm{K}_{\mathrm{E}} \qquad \frac{\Gamma \Rightarrow \Delta, \varphi, \varphi}{\Gamma \Rightarrow \Delta, \varphi}\ \mathrm{K}_{\mathrm{D}}$$

As regras de contração permitem que descartemos fórmulas redundantes do nosso estoque de fórmulas em um contexto.

(3) A regra estrutural de corte é

$$\frac{\Gamma \Rightarrow \Delta, \varphi \qquad \varphi, \Gamma' \Rightarrow \Delta'}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}\ \text{cut}$$

quaisquer que sejam os contextos Γ' e Δ'. A regra de corte é bem natural no seguinte sentido: provamos lemas e utilizamos tais lemas em provas de proposições, teoremas, etc. Intuitivamente, isto captura a prática de fazer desvios por subresultados antes de provar o resultado final.

Uma *prova* de um sequente $\Gamma \Rightarrow \Delta$ é uma árvore rotulada, finita e enraizada tal que cada vértice é rotulado por um sequente (em particular, a raíz é rotulada por $\Gamma \Rightarrow \Delta$), toda folha é rotulada por um sequente inicial ou por uma aplicação da regra $\bot_{\mathrm{E}}$ e os vértices que não são folhas são rotulados por sequentes que são conclusões de aplicações corretas de regras de dedução [13, 18]. O seguinte resultado pode ser provado por indução no comprimento das fórmulas utilizando as regras do sistema formal:

PROPOSIÇÃO III.1.8. Para cada fórmula φ, existe uma prova do sequente $\varphi, \Gamma \Rightarrow \Delta, \varphi$, quaisquer que sejam os contextos Γ e Δ.

Demonstração. O resultado é válido para fórmulas iniciais, pois neste caso a prova é simplesmente um sequente inicial. Suponhamos que o resultado seja válido para toda fórmula com comprimento menor que o de φ. Vamos supor que $\varphi = \exists x \psi(x)$ e vamos provar este caso para ilustrar o argumento por indução. Suponhamos que y seja uma variável que não ocorre em φ. A fórmula $\frac{y}{x}\psi(x)$ tem comprimento menor que o de φ. Da hipótese de indução, sabemos que existe uma prova π do sequente $\frac{y}{x}\psi(x) \Rightarrow \exists x \psi(x), \frac{y}{x}\psi(x)$. Obtemos então:

$$\dfrac{\dfrac{\begin{array}{c}\pi\\ \vdots\\ \frac{y}{x}\psi(x) \Rightarrow \exists x \psi(x), \frac{y}{x}\psi(x)\end{array}}{\frac{y}{x}\psi(x) \Rightarrow \exists x \psi(x)}\ \exists_{\mathrm{D}}}{\exists x \psi(x) \Rightarrow \exists x \psi(x)}\ \exists^{\bullet}_{\mathrm{E}}$$

Observemos que a variável y satisfaz a condição de autovariável da inferência $\exists^{\bullet}_{\mathrm{E}}$. Aplicando regras estruturais, podemos obter contextos arbitrários Γ e Δ, e portanto, obtemos uma prova do sequente $\exists x \psi(x), \Gamma \Rightarrow \Delta, \exists x \psi(x)$. Os demais casos são analisados de maneira análoga e o resultado segue do Princípio de Indução. ⊣

Poderíamos ter indicado também regras para os símbolos definidos $\neg$ e $\leftrightarrow$, como seguem. Observemos que as regras de dedução que regem os símbolos definidos $\neg$ e $\leftrightarrow$ podem ser derivadas das regras de dedução que regem as constantes lógicas $\bot$, $\wedge$, $\vee$ e $\rightarrow$.

(¬) As regras que regem o símbolo de negação ¬ são as regras $\neg_E$ e $\neg_D$ apresentadas na forma:

$$\dfrac{\Gamma \Rightarrow \Delta, \varphi}{\neg\varphi, \Gamma \Rightarrow \Delta}\ \neg_E \qquad \dfrac{\varphi, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\varphi}\ \neg_D$$

Suponhamos que existam provas π_1 e π_2 dos sequentes $\Gamma \Rightarrow \Delta, \varphi$ e $\varphi, \Gamma \Rightarrow \Delta$, respectivamente. As regras $\neg_E$ e $\neg_D$ podem ser derivadas das seguintes maneiras:

$$\dfrac{\pi_1 \quad \dfrac{}{\bot, \Gamma \Rightarrow \Delta}\ \bot_E}{\neg\varphi, \Gamma \Rightarrow \Delta}\ \to_E \qquad \dfrac{\dfrac{\pi_2}{\varphi, \Gamma \Rightarrow \Delta}\ W_D}{\Gamma \Rightarrow \Delta, \neg\varphi}\ \to_D$$

(↔) A regra que rege o símbolo de equivalência material ↔ é a regra $\leftrightarrow_D$ apresentada na forma:

$$\dfrac{\psi, \Gamma \Rightarrow \Delta, \phi \qquad \phi, \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \psi \leftrightarrow \phi}\ \leftrightarrow_D$$

Suponhamos que existam provas π_1 e π_2 dos sequentes $\psi, \Gamma \Rightarrow \Delta, \phi$ e $\phi, \Gamma \Rightarrow \Delta, \psi$, respectivamente. A regra $\leftrightarrow_D$ pode ser derivada da seguinte maneira:

$$\dfrac{\dfrac{\pi_1}{\psi, \Gamma \Rightarrow \Delta, \phi}\ \to_D}{\Gamma \Rightarrow \Delta, \psi \to \phi} \qquad \dfrac{\dfrac{\pi_2}{\phi, \Gamma \Rightarrow \Delta, \psi}\ \to_D}{\Gamma \Rightarrow \Delta, \phi \to \psi}$$
$$\dfrac{\Gamma \Rightarrow \Delta, \psi \to \phi \qquad \Gamma \Rightarrow \Delta, \phi \to \psi}{\Gamma \Rightarrow \Delta, \psi \leftrightarrow \phi}\ \wedge_D$$

Dizemos que uma fórmula φ é um *teorema* e escrevemos $\vdash \varphi$ quando existe uma prova do sequente $\Rightarrow \varphi$. O Exemplo III.1.9 a seguir mostra que certos princípios clássicos são teoremas do sistema de dedução aqui apresentado.

EXEMPLO III.1.9 (Teoremas). Este exemplo servirá para mostrar que o sistema formal apresentado é clássico, no sentido de derivar teoremas de lógica clássica como a eliminação da dupla negação.

(1) O princípio da não contradição é um teorema, isto é, $\vdash \neg(\neg\varphi \wedge \varphi)$. Dada uma fórmula φ, sabemos da Proposição III.1.8 que existe uma prova π de $\varphi \Rightarrow \varphi$. Obtemos:

$$\dfrac{\dfrac{\dfrac{\dfrac{\pi}{\vdots}}{\varphi \Rightarrow \varphi}}{\neg\varphi, \varphi \Rightarrow}\,\neg_{\mathrm{E}}}{\neg\varphi \wedge \varphi \Rightarrow}\,\wedge_{\mathrm{E}}}{\Rightarrow \neg(\neg\varphi \wedge \varphi)}\,\neg_{\mathrm{D}}$$

(2) O princípio do terceiro excluído é um teorema, isto é, $\vdash \neg\varphi \vee \varphi$. Dada uma fórmula φ, sabemos da Proposição III.1.8 que existe uma prova π de $\varphi \Rightarrow \varphi$. Obtemos:

$$\dfrac{\dfrac{\dfrac{\dfrac{\pi}{\vdots}}{\varphi \Rightarrow \varphi}}{\Rightarrow \varphi, \neg\varphi}\,\neg_{\mathrm{D}}}{\Rightarrow \varphi \vee \neg\varphi}\,\vee_{\mathrm{D}}$$

(3) A eliminação da dupla negação é um teorema, isto é, $\vdash \varphi \leftrightarrow \neg\neg\varphi$. Dada uma fórmula φ, sabemos da Proposição III.1.8 que existe uma prova π de $\varphi \Rightarrow \varphi$. Obtemos:

$$\dfrac{\dfrac{\dfrac{\dfrac{\pi}{\vdots}}{\varphi \Rightarrow \varphi}}{\neg\varphi, \varphi \Rightarrow}\,\neg_{\mathrm{E}}}{\varphi \Rightarrow \neg\neg\varphi}\,\neg_{\mathrm{D}} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\pi}{\vdots}}{\varphi \Rightarrow \varphi}}{\Rightarrow \varphi, \neg\varphi}\,\neg_{\mathrm{D}}}{\neg\neg\varphi \Rightarrow \varphi}\,\neg_{\mathrm{E}}}{\Rightarrow \varphi \leftrightarrow \neg\neg\varphi}\,\leftrightarrow_{\mathrm{D}}$$

(4) A regra *modus ponens* dos sistemas de Hilbert-Ackermann (como aquele apresentado por L. Halbeisen e R. Krapf [5]) é essencialmente o conteúdo do sequente $\psi \to \phi, \psi \Rightarrow \phi$, que sempre pode ser provado no atual sistema. Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 de $\psi \Rightarrow \phi, \psi$ e $\phi, \psi \Rightarrow \phi$, respectivamente. Obtemos:

$$\dfrac{\dfrac{\pi_1}{\vdots} \qquad \dfrac{\pi_2}{\vdots}}{\psi \Rightarrow \phi, \psi \qquad \phi, \psi \Rightarrow \phi}\,\to_{\mathrm{E}}}{\psi \to \phi, \psi \Rightarrow \phi}$$

(5) Vale a interdefinibilidade dos quantificadores, isto é, $\vdash \forall x\varphi(x) \leftrightarrow \neg\exists x\neg\varphi(x)$. Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 de $\frac{y}{x}\varphi(x), \forall x\varphi(x) \Rightarrow \frac{y}{x}\varphi(x)$ e $\frac{z}{x}\varphi(x) \Rightarrow \exists x\neg\varphi(x), \frac{z}{x}\varphi(x)$, respectivamente, de modo que as variáveis y e z não ocorrem em $\forall x\varphi(x)$ ou em $\exists x\varphi(x)$. Obtemos:

$$
\begin{prooftree}
\AxiomC{π_1}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\tfrac{y}{x}\varphi(x), \forall x\varphi(x) \Rightarrow \tfrac{y}{x}\varphi(x)$}
\RightLabel{$\forall_E$}
\UnaryInfC{$\forall x\varphi(x) \Rightarrow \tfrac{y}{x}\varphi(x)$}
\RightLabel{$\neg_E$}
\UnaryInfC{$\tfrac{y}{x}\neg\varphi(x), \forall x\varphi(x) \Rightarrow$}
\RightLabel{$\exists_E^\bullet$}
\UnaryInfC{$\exists x\neg\varphi(x), \forall x\varphi(x) \Rightarrow$}
\RightLabel{$\neg_D$}
\UnaryInfC{$\forall x\varphi(x) \Rightarrow \neg\exists x\neg\varphi(x)$}
\AxiomC{π_2}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\tfrac{z}{x}\varphi(x) \Rightarrow \exists x\neg\varphi(x), \tfrac{z}{x}\varphi(x)$}
\RightLabel{$\neg_D$}
\UnaryInfC{$\Rightarrow \exists x\neg\varphi(x), \tfrac{z}{x}\neg\varphi(x), \tfrac{z}{x}\varphi(x)$}
\RightLabel{$\exists_D$}
\UnaryInfC{$\Rightarrow \tfrac{z}{x}\varphi(x), \exists x\neg\varphi(x)$}
\RightLabel{$\neg_E$}
\UnaryInfC{$\neg\exists x\neg\varphi(x) \Rightarrow \tfrac{z}{x}\varphi(x)$}
\RightLabel{$\forall_D^\bullet$}
\UnaryInfC{$\neg\exists x\neg\varphi(x) \Rightarrow \forall x\varphi(x)$}
\RightLabel{$\leftrightarrow_D$}
\BinaryInfC{$\Rightarrow \forall x\varphi(x) \leftrightarrow \neg\exists x\neg\varphi(x)$}
\end{prooftree}
$$

(6) Vale sempre $\vdash (\psi \to \phi) \leftrightarrow (\neg\psi \vee \phi)$. Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 de $\psi \Rightarrow \phi, \psi$ e $\phi, \psi \Rightarrow \phi$, respectivamente. Obtemos:

$$
\begin{prooftree}
\AxiomC{π_1}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\psi \Rightarrow \phi, \psi$}
\AxiomC{π_2}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\phi, \psi \Rightarrow \phi$}
\RightLabel{$\to_E$}
\BinaryInfC{$\psi \to \phi, \psi \Rightarrow \phi$}
\RightLabel{$\neg_D$}
\UnaryInfC{$\psi \to \phi \Rightarrow \neg\psi, \phi$}
\RightLabel{$\vee_D$}
\UnaryInfC{$\psi \to \phi \Rightarrow \neg\psi \vee \phi$}
\AxiomC{π_1}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\psi \Rightarrow \phi, \psi$}
\RightLabel{$\neg_E$}
\UnaryInfC{$\neg\psi, \psi \Rightarrow \phi$}
\AxiomC{π_2}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\phi, \psi \Rightarrow \phi$}
\RightLabel{$\vee_E$}
\BinaryInfC{$\neg\psi \vee \phi, \psi \Rightarrow \phi$}
\RightLabel{$\to_D$}
\UnaryInfC{$\neg\psi \vee \phi \Rightarrow \psi \to \phi$}
\RightLabel{$\leftrightarrow_D$}
\BinaryInfC{$\Rightarrow (\psi \to \phi) \leftrightarrow (\neg\psi \vee \phi)$}
\end{prooftree}
$$

Estes resultados mostram que o sistema de dedução é clássico. ⊣

Dizemos que duas fórmulas ψ e ϕ são *sintaticamente equivalentes* quando $\vdash \psi \leftrightarrow \phi$. Por exemplo, o último item do Exemplo III.1.9 mostra que as fórmulas $\psi \to \phi$ e $\neg\psi \vee \phi$ são sintaticamente equivalentes. O exemplo a seguir apresenta mais casos de fórmulas sintaticamente equivalentes que serão bem úteis para o entendimento das propriedades sintáticas do sistema formal.

EXEMPLO III.1.10 (Equivalência Sintática). Apresentaremos neste exemplo casos importantes de equivalência sintática. Este exemplo mostra como podemos obter fórmulas sintaticamente equivalentes partindo de fórmulas sintaticamente equivalentes. Isto é feito por meio das regras de dedução, que descrevem o significado dos símbolos lógicos segundo o papel que eles desempenham em uma dedução. Os resultados deste exemplo servirão de motivação bem natural para o Teorema III.1.11. Suponhamos que α e β sejam fórmulas. Primeiro, observemos que se $\vdash \alpha \leftrightarrow \beta$, então existem provas de $\alpha, \Gamma \Rightarrow \Delta, \beta$ e $\beta, \Gamma \Rightarrow \Delta, \alpha$, onde Γ e Δ são contextos quaisquer. De fato, suponhamos que $\vdash \alpha \leftrightarrow \beta$. Existe uma prova π do sequente $\Gamma \Rightarrow \Delta, \alpha \leftrightarrow \beta$. Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 dos sequentes $\alpha, \beta \to \alpha, \Gamma \Rightarrow \Delta, \beta, \alpha$ e $\beta, \alpha, \beta \to \alpha, \Gamma \Rightarrow \Delta, \beta$, respectivamente. Disto, obtemos a seguinte prova do sequente $\alpha, \Gamma \Rightarrow \Delta, \beta$:

$$\dfrac{\dfrac{\pi \quad \dfrac{\pi_1 \qquad\qquad \pi_2}{\alpha, \beta \to \alpha, \Gamma \Rightarrow \Delta, \beta, \alpha \qquad \beta, \alpha, \beta \to \alpha, \Gamma \Rightarrow \Delta, \beta}\,{\to_E}}{\alpha \to \beta, \beta \to \alpha, \alpha, \Gamma \Rightarrow \Delta, \beta}\,{\wedge_E}}{\Gamma \Rightarrow \Delta, \alpha \leftrightarrow \beta \qquad \alpha \leftrightarrow \beta, \alpha, \Gamma \Rightarrow \Delta, \beta}\,{\text{cut}}$$
$$\alpha, \Gamma \Rightarrow \Delta, \beta$$

Raciocínio análogo para o sequente $\beta, \Gamma \Rightarrow \Delta, \alpha$. Isso que acabamos de mostrar permite provar os seguintes resultados com mais facilidade:

(1) Se $\vdash \alpha \leftrightarrow \beta$, então $\vdash \phi \vee \alpha \leftrightarrow \phi \vee \beta$. Suponhamos que $\vdash \alpha \leftrightarrow \beta$. Existem provas π_1 e π_2 dos sequentes $\alpha \Rightarrow \phi, \beta$ e $\beta \Rightarrow \phi, \alpha$, respectivamente. Da Proposição III.1.8, sabemos que existem provas π_3 e π_4 dos sequentes $\phi \Rightarrow \phi, \beta$ e $\phi \Rightarrow \phi, \alpha$, respectivamente. Obtemos a seguinte prova de $\Rightarrow \phi \vee \alpha \leftrightarrow \phi \vee \beta$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\pi_1 \qquad \pi_3}{\alpha \Rightarrow \phi, \beta \qquad \phi \Rightarrow \phi, \beta}\,{\vee_E}}{\phi \vee \alpha \Rightarrow \phi, \beta}\,{\vee_D}}{\phi \vee \alpha \Rightarrow \phi \vee \beta} \qquad \dfrac{\dfrac{\dfrac{\pi_2 \qquad \pi_4}{\beta \Rightarrow \phi, \alpha \qquad \phi \Rightarrow \phi, \alpha}\,{\vee_E}}{\phi \vee \beta \Rightarrow \phi, \alpha}\,{\vee_D}}{\phi \vee \beta \Rightarrow \phi \vee \alpha}}{\Rightarrow \phi \vee \alpha \leftrightarrow \phi \vee \beta}\,{\leftrightarrow_D}$$

(2) Se $\vdash \alpha \leftrightarrow \beta$, então $\vdash \alpha \vee \phi \leftrightarrow \beta \vee \phi$. Obtemos isto por meio de um raciocínio análogo ao do item anterior.

(3) Se $\vdash \alpha \leftrightarrow \beta$, então $\vdash \phi \wedge \alpha \leftrightarrow \phi \wedge \beta$. Suponhamos que $\vdash \alpha \leftrightarrow \beta$. Existem provas π_1 e π_2 dos sequentes $\phi, \alpha \Rightarrow \beta$ e $\phi, \beta \Rightarrow \alpha$, respectivamente. Da Proposição III.1.8, sabemos que existem provas π_3 e π_4 dos sequentes $\phi, \beta \Rightarrow \phi$ e $\phi, \alpha \Rightarrow \phi$, respectivamente. Obtemos a seguinte prova de $\Rightarrow \phi \wedge \alpha \leftrightarrow \phi \wedge \beta$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\pi_4 \qquad \pi_1}{\phi, \alpha \Rightarrow \phi \qquad \phi, \alpha \Rightarrow \beta}\,{\wedge_D}}{\phi, \alpha \Rightarrow \phi \wedge \beta}\,{\wedge_E}}{\phi \wedge \alpha \Rightarrow \phi \wedge \beta} \qquad \dfrac{\dfrac{\dfrac{\pi_3 \qquad \pi_2}{\phi, \beta \Rightarrow \phi \qquad \phi, \beta \Rightarrow \alpha}\,{\wedge_D}}{\phi, \beta \Rightarrow \phi \wedge \alpha}\,{\wedge_E}}{\phi \wedge \beta \Rightarrow \phi \wedge \alpha}}{\Rightarrow \phi \wedge \alpha \leftrightarrow \phi \wedge \beta}\,{\leftrightarrow_D}$$

(4) Se $\vdash \alpha \leftrightarrow \beta$, então $\vdash \alpha \wedge \phi \leftrightarrow \beta \wedge \phi$. Obtemos isto por meio de um raciocínio análogo ao do item anterior.

(5) Se $\vdash \alpha \leftrightarrow \beta$, então $\vdash (\phi \to \alpha) \leftrightarrow (\phi \to \beta)$. Suponhamos que $\vdash \alpha \leftrightarrow \beta$. Existem provas π_1 e π_2 dos sequentes $\alpha, \phi \Rightarrow \beta$ e $\beta, \phi \Rightarrow \alpha$, respectivamente. Da Proposição III.1.8, sabemos que existem provas π_3 e π_4 dos sequentes $\phi \Rightarrow \beta, \phi$ e $\phi \Rightarrow \alpha, \phi$, respectivamente. Obtemos a seguinte prova de $\Rightarrow \phi \to \alpha \leftrightarrow \phi \to \beta$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\pi_3 \qquad \pi_1}{\phi \Rightarrow \beta, \phi \qquad \alpha, \phi \Rightarrow \beta}\,{\to_E} \qquad \dfrac{\pi_4 \qquad \pi_2}{\phi \Rightarrow \alpha, \phi \qquad \beta, \phi \Rightarrow \alpha}\,{\to_E}}{\phi, \phi \to \alpha \Rightarrow \beta}\,{\to_D} \qquad \dfrac{}{\phi, \phi \to \beta \Rightarrow \alpha}\,{\to_D}}{\phi \to \alpha \Rightarrow \phi \to \beta} \qquad \dfrac{}{\phi \to \beta \Rightarrow \phi \to \alpha}}{\Rightarrow (\phi \to \alpha) \leftrightarrow (\phi \to \beta)}\,{\leftrightarrow_D}$$

(6) Se $\vdash \alpha \leftrightarrow \beta$, então $\vdash (\alpha \to \phi) \leftrightarrow (\beta \to \phi)$. Obtemos isto por meio de um raciocínio análogo ao do item anterior. ⊣⊢

O Teorema III.1.11 a seguir é uma adaptação para a presente linguagem do Teorema da Equivalência provado por J. Shoenfield [17]. O teorema mostra que quando substituímos fórmulas sintaticamente equivalentes em uma fórmula, obtemos uma fórmula sintaticamente equivalente à fórmula original.

TEOREMA III.1.11 (Equivalência). Suponhamos que a fórmula ψ seja obtida da fórmula φ pela substituição de algumas ocorrências das fórmulas $\alpha_1, \ldots, \alpha_m$ pelas fórmulas $\beta_1, \ldots, \beta_m$, respectivamente. Se $\vdash \alpha_i \leftrightarrow \beta_i$ para todo $i \in \{1, \ldots, m\}$, então $\vdash \varphi \leftrightarrow \psi$.

Demonstração. Suponhamos que para algum $j \in \{1, \ldots, m\}$ exista apenas uma ocorrência de α_j em φ e que ela seja a própria φ. Neste caso, vemos que $\varphi = \alpha_j$ e $\psi = \beta_j$. Da hipótese $\vdash \alpha_i \leftrightarrow \beta_i$ para todo $i \in \{1, \ldots, m\}$, obtemos $\vdash \varphi \leftrightarrow \psi$. Vamos provar o resultado por indução no comprimento de φ. Se φ é inicial, então segue do Teorema III.1.5 que toda ocorrência de uma fórmula em φ é toda φ. Se para algum $j \in \{1, \ldots, m\}$ existe uma ocorrência de α_j em φ, então segue do que provamos no início da demonstração que $\vdash \varphi \leftrightarrow \psi$. Se nenhuma $\alpha_1, \ldots, \alpha_m$ ocorre em φ, então $\varphi = \psi$, e portanto, $\vdash \varphi \leftrightarrow \psi$. Vamos agora seguir para os casos em que φ não é inicial. Suponhamos que o resultado seja válido para toda fórmula γ cujo comprimento é menor que o de φ.

(1) No primeiro caso, vamos supor que φ é $\wedge\alpha\beta$. Do Teorema III.1.5, sabemos que toda ocorrência de uma fórmula em φ ou é toda φ ou é parte de α ou β. Sabemos que os comprimentos de α e de β são menores que o de φ. Supondo que a ocorrência não seja toda a φ, usamos a hipótese de indução para α ou β e obtemos $\vdash \varphi \leftrightarrow \psi$.

(2) Os demais casos são demonstrados de maneira análoga ao caso anterior.

Do Princípio de Indução, obtemos o resultado. ⊣

Em uma fórmula da forma $\square\psi\phi$, dizemos que as fórmulas ψ e ϕ são o escopo do conectivo lógico binário $\square$. Dizemos que uma fórmula φ está na *forma normal*

prenex quando nenhum símbolo de quantificador em φ ocorre no escopo de um conectivo lógico binário. Em outras palavras, a fórmula φ é da forma

$$Q_m x_m \cdots Q_1 x_1 \psi(x_1, \ldots, x_m),$$

onde Q_1, ..., Q_m são quantificadores e $\psi(x_1, \ldots, x_m)$ é um fórmula livre de quantificadores na qual todas as variáveis são distintas [10, 13, 17, 18]. Observemos que as variáveis x_1, ..., x_m indicadas não são necessariamente as únicas variáveis que ocorrem em φ. Por outro lado, elas são necessariamente as únicas variáveis ligadas que ocorrem em φ, uma vez que ela está na forma normal prenex. Até agora, lidamos com regras de formação e dedução, mas é possível também estabelecer certas regras de reescrita de fórmulas. Vamos mostrar como reescrever uma fórmula para obter uma nova fórmula em forma normal prenex que é sintaticamente equivalente à fórmula original. Vamos adotar as seguintes regras de reescrita chamadas de *operações prenex*:

(1) Substituir ocorrências da fórmula $Qx\alpha(x)$ na fórmula φ por $Qy\alpha(y)$, desde que y não ocorra em φ.

(2) Substituir ocorrências das fórmulas $\wedge Qx\alpha(x)\beta$ e $\vee Qx\alpha(x)\beta$ na fórmula φ por $Qx \wedge \alpha(x)\beta$ e $Qx \vee \alpha(x)\beta$, respectivamente, desde que x não ocorra em β.[c]

(3) Substituir ocorrências da fórmula $\rightarrow Qx\alpha(x)\beta$ na fórmula φ por $Q^*x \rightarrow \alpha(x)\beta$, desde que x não ocorra em β.[d]

A intuição da primeira operação prenex é a seguinte: podemos mudar os nomes de variáveis ligadas utilizando novos nomes de variáveis. Verifiquemos que esta operação preserva o sentido das fórmulas. Suponhamos que $\alpha(x)$ seja uma fórmula e que y e z sejam variáveis distintas que não ocorrem em $\alpha(x)$. Podemos formar $\alpha(y) = \frac{y}{x}\alpha(x)$. Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 dos sequentes $\frac{z}{x}\alpha(x) \Rightarrow \exists y\alpha(y), \frac{z}{y}\alpha(y)$ e $\frac{z}{y}\alpha(y), \exists x\alpha(x) \Rightarrow \exists x\alpha(x), \frac{z}{x}\alpha(x)$. Vale $\vdash \exists x\alpha(x) \leftrightarrow \exists y\alpha(y)$. De fato:

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\pi_2\\ \vdots \\ \frac{z}{x}\alpha(x) \Rightarrow \exists y\alpha(y), \frac{z}{y}\alpha(y)\end{array}}{\frac{z}{x}\alpha(x) \Rightarrow \exists y\alpha(y)}\,\exists_{\mathrm{D}}}{\exists x\alpha(x) \Rightarrow \exists y\alpha(y)}\,\exists^{\bullet}_{\mathrm{E}} \qquad \dfrac{\dfrac{\dfrac{\begin{array}{c}\pi_2\\ \vdots \\ \frac{z}{y}\alpha(y) \Rightarrow \exists x\alpha(x), \frac{z}{x}\alpha(x)\end{array}}{\frac{z}{y}\alpha(y) \Rightarrow \exists x\alpha(x)}\,\exists_{\mathrm{D}}}{\exists y\alpha(y) \Rightarrow \exists x\alpha(x)}\,\exists^{\bullet}_{\mathrm{E}}}{\Rightarrow \exists x\alpha(x) \leftrightarrow \exists y\alpha(y)}\,\leftrightarrow_{\mathrm{D}}$$

Utilizando um raciocínio análogo, é possível mostrar que $\vdash \forall x\alpha(x) \leftrightarrow \forall y\alpha(y)$. O seguinte exemplo mostra resultados de equivalência sintática que servirão para demonstrar a corretude das operações prenex como aplicação do Teorema III.1.11.

[c] Usando abreviações: substituir $Qx\alpha(x) \wedge \beta$ e $Qx\alpha(x) \vee \beta$ por $Qx(\alpha(x) \wedge \beta)$ e $Qx(\alpha(x) \vee \beta)$, respectivamente, desde que x não ocorra em β.

[d] Usando abreviações: substituir $Qx\alpha(x) \rightarrow \beta$ por $Q^*x(\alpha(x) \rightarrow \beta)$, desde que x não ocorra em β.

EXEMPLO III.1.12 (Operações Prenex). Apresentaremos neste exemplo casos importantes de equivalência sintática que motivam a proposição das operações prenex. Tomemos as fórmulas $\alpha(x)$ e β de modo que x não ocorra em β. Vamos utilizar novas variáveis auxiliares para demonstrar a corretude do processo descrito pelas operações prenex. Suponhamos que y e z sejam variáveis que não ocorrem em $\alpha(x)$ ou β.

(1) Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 dos sequentes $\frac{y}{x}\alpha(x) \Rightarrow \exists x(\alpha(x) \vee \beta), \frac{y}{x}\alpha(x), \beta$ e $\beta \Rightarrow \exists x(\alpha(x) \vee \beta), \frac{z}{x}\alpha(x), \beta$, respectivamente. Obtemos a seguinte prova de $\exists x\alpha(x) \vee \beta \Rightarrow \exists x(\alpha(x) \vee \beta)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\pi_1}{\frac{y}{x}\alpha(x) \Rightarrow \exists x(\alpha(x) \vee \beta), \frac{y}{x}\alpha(x), \beta}\,\vee_D}{\frac{y}{x}\alpha(x) \Rightarrow \exists x(\alpha(x) \vee \beta), \frac{y}{x}(\alpha(x) \vee \beta)}\,\exists_D}{\frac{y}{x}\alpha(x) \Rightarrow \exists x(\alpha(x) \vee \beta)}\,\exists^{\bullet}_E}{\exists x\alpha(x) \Rightarrow \exists x(\alpha(x) \vee \beta)} \qquad \dfrac{\dfrac{\dfrac{\pi_2}{\beta \Rightarrow \exists x(\alpha(x) \vee \beta), \frac{z}{x}\alpha(x), \beta}\,\vee_D}{\beta \Rightarrow \exists x(\alpha(x) \vee \beta), \frac{z}{x}(\alpha(x) \vee \beta)}\,\exists_D}{\beta \Rightarrow \exists x(\alpha(x) \vee \beta)}}{\exists x\alpha(x) \vee \beta \Rightarrow \exists x(\alpha(x) \vee \beta)}\,\vee_E$$

(2) Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 dos sequentes $\frac{y}{x}\alpha(x) \Rightarrow \exists x\alpha(x), \frac{y}{x}\alpha(x), \beta$ e $\beta \Rightarrow \exists x\alpha(x), \frac{z}{x}\alpha(x), \beta$, respectivamente. Obtemos a seguinte prova de $\exists x(\alpha(x) \vee \beta) \Rightarrow \exists x\alpha(x) \vee \beta$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\pi_1}{\frac{y}{x}\alpha(x) \Rightarrow \exists x\alpha(x), \frac{y}{x}\alpha(x), \beta}\,\exists_D}{\frac{y}{x}\alpha(x) \Rightarrow \exists x\alpha(x), \beta}\,\vee_D}{\frac{y}{x}\alpha(x) \Rightarrow \exists x\alpha(x) \vee \beta} \qquad \dfrac{\dfrac{\dfrac{\pi_2}{\beta \Rightarrow \exists x\alpha(x), \frac{z}{x}\alpha(x), \beta}\,\exists_D}{\beta \Rightarrow \exists x\alpha(x), \beta}\,\vee_D}{\beta \Rightarrow \exists x\alpha(x) \vee \beta}}{\frac{y}{x}(\alpha(x) \vee \beta) \Rightarrow \exists x\alpha(x) \vee \beta}\,\vee_E}{\exists x(\alpha(x) \vee \beta) \Rightarrow \exists x\alpha(x) \vee \beta}\,\exists^{\bullet}_E$$

(3) Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 dos sequentes $\frac{y}{x}\alpha(x), \beta \Rightarrow \exists x(\alpha(x) \wedge \beta), \frac{y}{x}\alpha(x)$ e $\frac{y}{x}\alpha(x), \beta \Rightarrow \exists x(\alpha(x) \wedge \beta), \beta$, respectivamente. Obtemos a seguinte prova de $\exists x(\alpha(x) \wedge \beta) \Rightarrow \exists x\alpha(x) \wedge \beta$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\pi_1}{\vdots}}{\frac{y}{x}\alpha(x), \beta \Rightarrow \exists x(\alpha(x) \wedge \beta), \frac{y}{x}\alpha(x)} \quad \dfrac{\dfrac{\pi_2}{\vdots}}{\frac{y}{x}\alpha(x), \beta \Rightarrow \exists x(\alpha(x) \wedge \beta), \beta}}{\dfrac{\frac{y}{x}\alpha(x), \beta \Rightarrow \exists x(\alpha(x) \wedge \beta), \frac{y}{x}(\alpha(x) \wedge \beta)}{\frac{y}{x}\alpha(x), \beta \Rightarrow \exists x(\alpha(x) \wedge \beta)}\,\exists_{\mathrm{D}}}\,\wedge_{\mathrm{D}}}{\exists x\alpha(x), \beta \Rightarrow \exists x(\alpha(x) \wedge \beta)}\,\exists^{\bullet}_{\mathrm{E}}}{\exists x\alpha(x) \wedge \beta \Rightarrow \exists x(\alpha(x) \wedge \beta)}\,\wedge_{\mathrm{E}}$$

(4) Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 dos sequentes $\frac{y}{x}\alpha(x), \beta \Rightarrow \exists x\alpha(x), \frac{y}{x}\alpha(x)$ e $\frac{y}{x}\alpha(x), \beta \Rightarrow \beta$, respectivamente. Obtemos a seguinte prova de $\exists x(\alpha(x) \wedge \beta) \Rightarrow \exists x\alpha(x) \wedge \beta$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\pi_1}{\vdots}}{\frac{y}{x}\alpha(x), \beta \Rightarrow \exists x\alpha(x), \frac{y}{x}\alpha(x)}\,\exists_{\mathrm{D}} \quad \dfrac{\pi_2}{\vdots}}{\frac{y}{x}\alpha(x), \beta \Rightarrow \exists x\alpha(x) \quad \frac{y}{x}\alpha(x), \beta \Rightarrow \beta}\,\wedge_{\mathrm{D}}}{\frac{y}{x}\alpha(x), \beta \Rightarrow \exists x\alpha(x) \wedge \beta}\,\wedge_{\mathrm{E}}}{\frac{y}{x}(\alpha(x) \wedge \beta) \Rightarrow \exists x\alpha(x) \wedge \beta}\,\exists^{\bullet}_{\mathrm{E}}}{\exists x(\alpha(x) \wedge \beta) \Rightarrow \exists x\alpha(x) \wedge \beta}$$

(5) Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 dos sequentes $\frac{y}{x}\alpha(x), \forall x\alpha(x) \Rightarrow \frac{y}{x}\alpha(x), \beta$ e $\beta \Rightarrow \frac{y}{x}\alpha(x), \beta$, respectivamente. Obtemos a seguinte prova de $\forall x\alpha(x) \vee \beta \Rightarrow \forall x(\alpha(x) \vee \beta)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\pi_1}{\vdots}}{\frac{y}{x}\alpha(x), \forall x\alpha(x) \Rightarrow \frac{y}{x}\alpha(x), \beta}\,\forall_{\mathrm{E}} \quad \dfrac{\pi_2}{\vdots}}{\forall x\alpha(x) \Rightarrow \frac{y}{x}\alpha(x), \beta \quad \beta \Rightarrow \frac{y}{x}\alpha(x), \beta}\,\vee_{\mathrm{E}}}{\forall x\alpha(x) \vee \beta \Rightarrow \frac{y}{x}\alpha(x), \beta}\,\vee_{\mathrm{D}}}{\forall x\alpha(x) \vee \beta \Rightarrow \frac{y}{x}(\alpha(x) \vee \beta)}\,\forall^{\bullet}_{\mathrm{D}}}{\forall x\alpha(x) \vee \beta \Rightarrow \forall x(\alpha(x) \vee \beta)}$$

(6) Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 dos sequentes $\frac{y}{x}\alpha(x)$, $\forall x(\alpha(x) \vee \beta) \Rightarrow \frac{y}{x}\alpha(x), \beta$ e $\beta, \forall x(\alpha(x) \vee \beta) \Rightarrow \frac{y}{x}\alpha(x), \beta$, respectivamente. Obtemos a seguinte prova de $\forall x(\alpha(x) \vee \beta) \Rightarrow \forall x\alpha(x) \vee \beta$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\pi_1 \qquad\qquad \pi_2}{\frac{y}{x}\alpha(x), \forall x(\alpha(x) \vee \beta) \Rightarrow \frac{y}{x}\alpha(x), \beta \qquad \beta, \forall x(\alpha(x) \vee \beta) \Rightarrow \frac{y}{x}\alpha(x), \beta}\vee_{\mathrm{E}}}{\frac{y}{x}(\alpha(x) \vee \beta), \forall x(\alpha(x) \vee \beta) \Rightarrow \frac{y}{x}\alpha(x), \beta}\forall_{\mathrm{E}}}{\forall x(\alpha(x) \vee \beta) \Rightarrow \frac{y}{x}\alpha(x), \beta}\forall^{\bullet}_{\mathrm{D}}}{\forall x(\alpha(x) \vee \beta) \Rightarrow \forall x\alpha(x), \beta}\vee_{\mathrm{D}}}{\forall x(\alpha(x) \vee \beta) \Rightarrow \forall x\alpha(x) \vee \beta}$$

(7) Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 dos sequentes $\frac{y}{x}\alpha(x)$, $\forall x\alpha(x), \beta \Rightarrow \frac{y}{x}\alpha(x)$ e $\frac{y}{x}\alpha(x), \forall x\alpha(x), \beta \Rightarrow \beta$, respectivamente. Obtemos a seguinte prova de $\forall x\alpha(x) \wedge \beta \Rightarrow \forall x(\alpha(x) \wedge \beta)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\pi_1 \qquad\qquad \pi_2}{\frac{y}{x}\alpha(x), \forall x\alpha(x), \beta \Rightarrow \frac{y}{x}\alpha(x) \qquad \frac{y}{x}\alpha(x), \forall x\alpha(x), \beta \Rightarrow \beta}\wedge_{\mathrm{D}}}{\frac{y}{x}\alpha(x), \forall x\alpha(x), \beta \Rightarrow \frac{y}{x}(\alpha(x) \wedge \beta)}\forall_{\mathrm{E}}}{\forall x\alpha(x), \beta \Rightarrow \frac{y}{x}(\alpha(x) \wedge \beta)}\wedge_{\mathrm{E}}}{\forall x\alpha(x) \wedge \beta \Rightarrow \frac{y}{x}(\alpha(x) \wedge \beta)}\forall^{\bullet}_{\mathrm{D}}}{\forall x\alpha(x) \wedge \beta \Rightarrow \forall x(\alpha(x) \wedge \beta)}$$

(8) Da Proposição III.1.8, sabemos que existem provas π_1 e π_2 dos sequentes $\frac{y}{x}\alpha(x), \beta$, $\forall x(\alpha(x) \wedge \beta) \Rightarrow \frac{y}{x}\alpha(x)$ e $\frac{z}{x}\alpha(x), \beta, \forall x(\alpha(x) \wedge \beta) \Rightarrow \beta$, respectivamente. Obtemos a seguinte prova de $\forall x(\alpha(x) \wedge \beta) \Rightarrow \forall x\alpha(x) \wedge \beta$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\pi_1}{\vdots}}{\frac{y}{x}\alpha(x), \beta, \forall x(\alpha(x) \wedge \beta) \Rightarrow \frac{y}{x}\alpha(x)}}{\frac{y}{x}(\alpha(x) \wedge \beta), \forall x(\alpha(x) \wedge \beta) \Rightarrow \frac{y}{x}\alpha(x)}\,\wedge_{\mathrm{E}}}{\forall x(\alpha(x) \wedge \beta) \Rightarrow \frac{y}{x}\alpha(x)}\,\forall_{\mathrm{E}}}{\forall x(\alpha(x) \wedge \beta) \Rightarrow \forall x\alpha(x)}\,\forall^{\bullet}_{\mathrm{D}} \qquad \dfrac{\dfrac{\dfrac{\pi_1}{\vdots}}{\frac{z}{x}\alpha(x), \beta, \forall x(\alpha(x) \wedge \beta) \Rightarrow \beta}}{\frac{z}{x}(\alpha(a) \wedge \beta), \forall x(\alpha(x) \wedge \beta) \Rightarrow \beta}\,\wedge_{\mathrm{E}}}{\forall x(\alpha(x) \wedge \beta) \Rightarrow \beta}\,\forall_{\mathrm{E}}}{\forall x(\alpha(x) \wedge \beta) \Rightarrow \forall x\alpha(x) \wedge \beta}\,\wedge_{\mathrm{D}}$$

⊣⊢

COROLÁRIO III.1.13. Dada uma fórmula φ, existe uma fórmula ψ na forma normal prenex tal que $\vdash \varphi \leftrightarrow \psi$.

A possibilidade de reescrever toda formula de $\mathrm{L_I}$ em forma normal prenex facilitará a análise semântica das propriedades de $\mathrm{L_I}$ e o estudo de compatibilidade de árvores na Seção III.5.

III.2 CORRETUDE E MODELOS

Até este ponto, focamos apenas nos aspectos sintáticos da linguagem $\mathrm{L_I}$. Nosso foco agora será descrever os aspectos básicos de sua semântica. Vamos apresentar uma semântica baseada no que foi feito por D. van Dalen [20] e J. Shoenfield [17]. Neste contexto, lidaremos com regras de interpretação da linguagem por estruturas de acordo com a semântica de Tarski. O Teorema III.2.3 apresenta a corretude do sistema de dedução apresentado nas seções anteriores. Finalizaremos esta seção com a apresentação da Teoria de Matroides na linguagem monádica de segunda ordem discutida, além de alguns resultados modelo-teóricos.

Uma *estrutura* para uma linguagem monádica de segunda ordem $\mathrm{L_I}$ é um par $\mathrm{M} = (\mathrm{E(M)}, \mathcal{I}(\mathrm{M}))$, no qual $\mathrm{E(M)}$ e $\mathcal{I}(\mathrm{M})$ são conjuntos finitos e não-vazios com $\mathcal{I}(\mathrm{M}) \subseteq 2^{\mathrm{E(M)}}$. Cada constante c é interpretada como um subconjunto de $\mathrm{E(M)}$. Para cada $\mathrm{X} \subseteq \mathrm{E(M)}$, tomemos um novo símbolo constante c_{X} chamado de *nome* de X de modo que nomes distintos correspondam a conjuntos distintos. Denotemos por $\mathrm{L} = \mathrm{L_I(M)}$ a extensão obtida de $\mathrm{L_I}$ pela adição dos nomes dos elementos de $2^{\mathrm{E(M)}}$ aos seus símbolos de constantes e por $\mathrm{Snt(L)}$ e $\mathrm{Cst(L)}$ os seus conjuntos de sentenças e de constantes, respectivamente. Uma *avaliação* de sentenças $\mathrm{M}[-]$ induzida por uma *interpretação*[e] de constantes $-^{\mathrm{M}}$ é uma função definida

[e] Vale observar aqui que esta semântica é diferente da semântica de linguagens de primeira ordem. Em uma linguagem de primeira ordem, interpretamos as constantes em uma estrutura como indivíduos (i.e. elementos do conjunto subjacente da estrutura). Já na linguagem objeto estudada nesta dissertação, nosso interesse é sobre conjuntos de indivíduos (i.e. elementos do conjunto das partes do conjunto subjacente da estrutura). Mais ainda, temos uma semântica *plena* para a linguagem objeto desta dissertação, i.e. não nos restrigimos a um subconjunto próprio do conjunto das partes para interpretar constantes ou descrever as interpretações dos quantificadores. Vide D. van Dalen [20] para mais detalhes sobre estas distinções.

recursivamente da seguinte maneira:

$$\begin{aligned} \mathrm{M}[-] : \mathrm{Snt}(\mathrm{L}) &\longrightarrow \{0,1\} & -^{\mathrm{M}} : \mathrm{Cst}(\mathrm{L}) &\longrightarrow 2^{\mathrm{E}(\mathrm{M})} \\ \varphi &\longmapsto \mathrm{M}[\varphi] & c &\longmapsto c^{\mathrm{M}} \\ & & c_{\mathrm{X}} &\longmapsto \mathrm{X} \end{aligned}$$

(1) Primeiro, definimos as avaliações para sentenças iniciais da linguagem L:

(1.1) $\mathrm{M}[\bot] = 0$.

(1.2) $\mathrm{M}[\mathrm{Sng}\, c] = 1$ sse $|c^{\mathrm{M}}| = 1$.

(1.3) $\mathrm{M}[\mathrm{Ind}\, c] = 1$ sse $c^{\mathrm{M}} \in \mathcal{I}(\mathrm{M})$.

(1.4) $\mathrm{M}[\sqsubseteq ck] = 1$ sse $c^{\mathrm{M}} \subseteq k^{\mathrm{M}}$.

(2) Uma vez definidas as avaliações para as sentenças iniciais da linguagem L, definimos as avaliações das sentenças da linguagem L recursivamente:

(2.1) $\mathrm{M}[\wedge\alpha\beta] = \min\{\, \mathrm{M}[\alpha], \mathrm{M}[\beta] \,\}$.

(2.2) $\mathrm{M}[\vee\alpha\beta] = \max\{\, \mathrm{M}[\alpha], \mathrm{M}[\beta] \,\}$.

(2.3) $\mathrm{M}[\rightarrow\alpha\beta] = \max\{\, 1 - \mathrm{M}[\alpha], \mathrm{M}[\beta] \,\}$.

(2.4) $\mathrm{M}[\exists x\varphi(x)] = \max\{\, \mathrm{M}[\frac{c_{\mathrm{X}}}{x}\varphi(x)] : \mathrm{X} \subseteq \mathrm{E}(\mathrm{M}) \,\}$.

(2.5) $\mathrm{M}[\forall x\varphi(x)] = \min\{\, \mathrm{M}[\frac{c_{\mathrm{X}}}{x}\varphi(x)] : \mathrm{X} \subseteq \mathrm{E}(\mathrm{M}) \,\}$.

Dizemos que uma sentença φ de L é *verdadeira*[f] e escrevemos $\mathrm{M} \models \varphi$ sse $\mathrm{M}[\varphi] = 1$. Neste caso, dizemos também que M é um *modelo* para φ. Dizemos que uma sentença φ de L_{I} é *válida* e escrevemos $\models \varphi$ sse φ é verdadeira em todas as estruturas. A seguinte proposição segue diretamente das regras descritas anteriormente:

PROPOSIÇÃO III.2.1. Dada uma estrutura M para L_{I}, tomemos $\mathrm{L} = \mathrm{L}_{\mathrm{I}}(\mathrm{M})$. Para todas sentenças α, β, $\exists x\varphi(x)$ e $\forall x\varphi(x)$ de L, temos:

(1) $\mathrm{M} \models \alpha \wedge \beta$ sse $\mathrm{M} \models \alpha$ e $\mathrm{M} \models \beta$.

(2) $\mathrm{M} \models \alpha \vee \beta$ sse $\mathrm{M} \models \alpha$ ou $\mathrm{M} \models \beta$.

(3) $\mathrm{M} \models \alpha \rightarrow \beta$ sse $\mathrm{M} \not\models \alpha$ ou $\mathrm{M} \models \beta$.

(4) $\mathrm{M} \models \exists x\varphi(x)$ sse para pelo menos um $\mathrm{X} \subseteq \mathrm{E}(\mathrm{M})$ vale $\mathrm{M} \models \varphi(c_{\mathrm{X}})$. Isto permite reduzir a quantificação existencial no contexto de estruturas finitas a uma disjunção finita, i.e. $\mathrm{M} \models \exists x\varphi(x)$ sse

$$\mathrm{M} \models \bigvee_{\mathrm{X} \subseteq \mathrm{E}(\mathrm{M})} \frac{c_{\mathrm{X}}}{x}\varphi(x).$$

(5) $\mathrm{M} \models \forall x\varphi(x)$ sse para todo $\mathrm{X} \subseteq \mathrm{E}(\mathrm{M})$ vale $\mathrm{M} \models \varphi(c_{\mathrm{X}})$. Isto permite reduzir a quantificação universal no contexto de estruturas finitas a uma conjunção finita, i.e. $\mathrm{M} \models \forall x\varphi(x)$ sse

$$\mathrm{M} \models \bigwedge_{\mathrm{X} \subseteq \mathrm{E}(\mathrm{M})} \frac{c_{\mathrm{X}}}{x}\varphi(x).$$

[f] A noção de verdade definida aqui é formal: poderíamos ter definido "φ é feliz em M", "φ é boa em M" ou mesmo "φ é verde em M" no lugar de "φ é verdadeira em M" e seguido com o estudo sistemático dos resultados sem problemas.

EXEMPLO III.2.2 (Expressividade). A linguagem $\mathrm{L_I}$ é capaz de expressar certos conceitos importantes. Tomemos uma estrutura M, definamos $\mathrm{U} = 2^{\mathrm{E(M)}}$ e formemos a linguagem $\mathrm{L} = \mathrm{L_I(M)}$. A linguagem $\mathrm{L_I}$ expressa uma relação $\mathrm{R} \subseteq \mathrm{U}^m$ sse existe uma fórmula φ de $\mathrm{L_I}$ cujas variáveis livres são exatamente $z_1, \ldots, z_m$ tal que para todo $(\mathrm{X}_1, \ldots, \mathrm{X}_m) \in \mathrm{U}^m$ vale $(\mathrm{X}_1, \ldots, \mathrm{X}_m) \in \mathrm{R}$ sse $\mathrm{M} \models \frac{c_{\mathrm{X}_1}, \ldots, c_{\mathrm{X}_m}}{z_1, \ldots, z_m} \varphi$. Vamos apresentar a seguir certas fórmulas que expressam certos conceitos.

(1) Podemos expressar em $\mathrm{L_I}$ a igualdade de conjuntos utilizando o símbolo $\sqsubseteq$. Vamos introduzir o símbolo $\doteq$ para indicar esta igualdade linguística e para diferenciá-la do símbolo de igualdade $=$ que usamos na metalinguagem. A fórmula de $\mathrm{L_I}$ que expressa igualdade de conjuntos é $(x \sqsubseteq y) \wedge (y \sqsubseteq x)$ e a abreviamos por $x \doteq y$. Verifiquemos que $x \doteq y$ realmente internaliza a noção de igualdade de conjuntos na linguagem $\mathrm{L_I}$. Dados uma estrutura M e conjuntos $\mathrm{X}, \mathrm{Y} \subseteq \mathrm{E(M)}$, sabemos que $\mathrm{X} = \mathrm{Y}$ sse $\mathrm{X} \subseteq \mathrm{Y}$ e $\mathrm{Y} \subseteq \mathrm{X}$. Isto é equivalente a $\mathrm{M} \models (c_{\mathrm{X}} \sqsubseteq c_{\mathrm{Y}}) \wedge (c_{\mathrm{Y}} \sqsubseteq c_{\mathrm{X}})$. Vemos então que $\mathrm{X} = \mathrm{Y}$ em M sse $\mathrm{M} \models c_{\mathrm{X}} \doteq c_{\mathrm{Y}}$.

(2) Podemos expressar em $\mathrm{L_I}$ a noção de conjunto independente $\subseteq$-maximal pela fórmula $(\mathrm{Ind}\, z) \wedge \forall x((\mathrm{Ind}\, x) \wedge ((z \sqsubseteq x) \to (x \sqsubseteq z)))$ que abreviamos por $\mathrm{Base}\, z$. Dado $\mathrm{X} \subseteq \mathrm{E(M)}$, temos $\mathrm{X} \in \mathcal{I}(\mathrm{M})$ maximal sse para todo $\mathrm{Y} \subseteq \mathrm{E(M)}$ se $\mathrm{Y} \in \mathcal{I}(\mathrm{M})$ e $\mathrm{X} \subseteq \mathrm{Y}$, então $\mathrm{Y} \subseteq \mathrm{X}$. Disto, vemos que $\mathrm{X} \subseteq \mathrm{E(M)}$ é independente $\subseteq$-maximal sse $\mathrm{M} \models \mathrm{Ind}\, c_{\mathrm{X}}$ e para todo $\mathrm{Y} \subseteq \mathrm{E(M)}$ se $\mathrm{M} \models \mathrm{Ind}\, c_{\mathrm{Y}}$ e $\mathrm{M} \models c_{\mathrm{X}} \sqsubseteq c_{\mathrm{Y}}$, então $\mathrm{M} \models c_{\mathrm{Y}} \sqsubseteq c_{\mathrm{X}}$. Isto é equivalente a $\mathrm{M} \models (\mathrm{Ind}\, c_{\mathrm{X}}) \wedge \forall x((\mathrm{Ind}\, x) \wedge ((c_{\mathrm{X}} \sqsubseteq x) \to (x \sqsubseteq c_{\mathrm{X}})))$. Vemos então que $\mathrm{X} \in \mathcal{I}(\mathrm{M})$ é $\subseteq$-maximal sse $\mathrm{M} \models \mathrm{Base}\, c_{\mathrm{X}}$.

(3) Podemos expressar em $\mathrm{L_I}$ a noção de que um conjunto é a união de um número finito fixado de conjuntos pela fórmula

$$\forall x((\mathrm{Sng}\, x) \to ((x \sqsubseteq z_{n+1}) \leftrightarrow ((x \sqsubseteq z_1) \vee \cdots \vee (x \sqsubseteq z_n)))),$$

que abreviamos por $\mathrm{Uni}_n\, z_1 \cdots z_n z_{n+1}$. Dado $\mathrm{X} \subseteq \mathrm{E(M)}$, suponhamos que $\mathrm{X} = \mathrm{X}_1 \cup \cdots \cup \mathrm{X}_n$. Dado $\mathrm{Y} \subseteq \mathrm{E(M)}$ com $|\mathrm{Y}| = 1$, temos $\mathrm{Y} \subseteq \mathrm{X}$ sse existe $i \in \{1, \ldots, n\}$ tal que $\mathrm{Y} \subseteq \mathrm{X}_i$. Vemos então que $\mathrm{X} = \mathrm{X}_1 \cup \cdots \cup \mathrm{X}_n$ sse $\mathrm{M} \models \mathrm{Uni}_n\, c_{\mathrm{X}_1} \cdots c_{\mathrm{X}_n} c_{\mathrm{X}}$.

(4) Dualizando o item anterior, podemos expressar em $\mathrm{L_I}$ a noção de que um conjunto é a interseção de um número finito de conjuntos pela fórmula

$$\forall x((\mathrm{Sng}\, x) \to ((x \sqsubseteq z_{n+1}) \leftrightarrow ((x \sqsubseteq z_1) \wedge \cdots \wedge (x \sqsubseteq z_n)))),$$

que abreviamos por $\mathrm{Int}_n\, z_1 \cdots z_n z_{n+1}$. A demonstração deste fato é análoga à do item anterior.

(5) Podemos expressar em $\mathrm{L_I}$ a noção de que um conjunto é a diferença de outros dois conjuntos pela fórmula

$$\forall x((\mathrm{Sng}\, x) \to ((x \sqsubseteq z) \leftrightarrow ((x \sqsubseteq z_1) \wedge (\neg x \sqsubseteq z_2)))),$$

que abreviamos por $\mathrm{Dif}\, z_1 z_2 z$. Dado $\mathrm{X} \subseteq \mathrm{E(M)}$, suponhamos que $\mathrm{Z} = \mathrm{X} - \mathrm{Y}$. Dado $\mathrm{A} \subseteq \mathrm{E(M)}$ com $|\mathrm{A}| = 1$, temos $\mathrm{A} \subseteq \mathrm{Z}$ sse $\mathrm{A} \subseteq \mathrm{X}$ e $\mathrm{A} \nsubseteq \mathrm{Y}$. Vemos então que $\mathrm{Z} = \mathrm{X} - \mathrm{Y}$ sse $\mathrm{M} \models \mathrm{Dif}\, c_{\mathrm{X}} c_{\mathrm{Y}} c_{\mathrm{Z}}$.

(6) Podemos expressar em $\mathrm{L_I}$ a noção de hereditariedade de conjuntos independentes pela fórmula $(\mathrm{Ind}\, y) \wedge ((x \sqsubseteq y) \to (\mathrm{Ind}\, x))$, que abreviamos por $\mathrm{Her}\, xy$.

(7) Podemos expressar em $\mathrm{L_I}$ a propriedade de troca pela fórmula

$$\begin{aligned}&((\mathrm{Base}\, z_1) \wedge (\mathrm{Ind}\, z_2) \wedge (\neg\, \mathrm{Base}\, z_2)) \to \\ &\quad \exists x \exists y((\mathrm{Sng}\, x) \wedge (x \sqsubseteq z_1) \wedge (\neg x \sqsubseteq z_2) \wedge (\mathrm{Uni}_2\, z_2 x y) \wedge (\mathrm{Ind}\, y)),\end{aligned}$$

que abreviamos por $\mathrm{Exc}\, xy$. ⊣⊢

Até agora, lidamos com interpretações de sentenças e desejamos, a partir deste ponto, lidar com interpretações de sequentes. Um desafio que enfrentamos para alcançar este objetivo é o de definir interpretações para fórmulas e faremos isso como segue. Dados Γ e Δ multiconjuntos finitos de fórmulas de $\mathrm{L_I}$, denotemos por $\mathrm{Par}(\Gamma, \Delta)$ a união dos conjuntos de variáveis livres de cada fórmula ψ de $\mathrm{L_I}$ em Γ e Δ. Uma *atribuição* de Γ e Δ em uma estrutura M é uma função $\tau : \mathrm{Par}(\Gamma, \Delta) \longrightarrow 2^{\mathrm{E(M)}}$. Definimos Γ^τ e Δ^τ multiconjuntos de sentenças de $\mathrm{L} = \mathrm{L_I(M)}$ obtidas da substituição das variáveis livres nas fórmulas de Γ e Δ pelos nomes das suas imagens segundo a atribuição τ. Se Γ e Δ consistem apenas de sentenças, então $\Gamma^\tau = \Gamma$ e $\Delta^\tau = \Delta$. Lembremos da interpretação intuitiva de sequentes apresentada na Seção III.1: um sequente da forma $\alpha_1, \ldots, \alpha_m \Rightarrow \beta_1, \ldots, \beta_n$ significa "se $\alpha_1 \wedge \cdots \wedge \alpha_m$, então $\beta_1 \vee \cdots \vee \beta_n$". Seguindo esta motivação, escrevemos $\wedge\Gamma^\tau$ para denotar a conjunção de todas as sentenças de Γ^τ e escrevemos $\vee\Delta^\tau$ para denotar a disjunção de todas as sentenças de Δ^τ. Convencionamos $\wedge\Gamma^\tau = \top$ se Γ é vazio e $\vee\Delta^\tau = \bot$ se Δ é vazio. As sentenças $\wedge\Gamma^\tau$ e $\vee\Delta^\tau$ são bem-definidas, uma vez que os multiconjuntos são finitos. Além disso, estão bem-definidas as avaliações

$$\mathrm{M}[\wedge\Gamma^\tau] = \min\{\, \mathrm{M}[\varphi^\tau] : \varphi \in \Gamma \,\}$$
$$\mathrm{M}[\vee\Delta^\tau] = \max\{\, \mathrm{M}[\varphi^\tau] : \varphi \in \Delta \,\}$$

quando existem fórmulas em Γ e Δ. Observemos que a escolha de mínimos e máximos nessa definição é compatível com a semântica apresentada para os conectivos de conjunção e disjunção: basta que uma sentença seja falsa em uma conjunção para que a conjunção seja falsa e basta que uma sentença seja verdadeira em uma disjunção para que a disjunção seja verdadeira. Dizemos que um sequente $\Gamma \Rightarrow \Delta$ é *válido* sse para toda estrutura M e toda atribuição $\tau : \mathrm{Par}(\Gamma, \Delta) \longrightarrow 2^{\mathrm{E(M)}}$ vale $\mathrm{M}[\wedge\Gamma^\tau] \leq \mathrm{M}[\vee\Delta^\tau]$. Caso contrário, dizemos que o sequente é *inválido*. Observemos que isso é compatível com a interpretação intuitiva de sequentes quando analisamos a semântica apresentada para o conectivo de implicação: uma condicional $\alpha \to \beta$ é verdadeira sempre que seu antecedente α é falso ou seu sucedente β é verdadeiro. O Teorema[g] III.2.3 a seguir é uma adaptação para a presente linguagem do Teorema 3.3.5 feito por J. von Plato e S. Negri [13].

TEOREMA III.2.3 (Correção). Se existe uma prova de $\Gamma \Rightarrow \Delta$, então $\Gamma \Rightarrow \Delta$ é válido.

Demonstração. A demonstração é feita por indução no número de regras utilizadas na prova de $\Gamma \Rightarrow \Delta$. ⊣

O Teorema III.2.3 é importante, pois ele evidencia que o sistema de dedução apresentado tem utilidade: se existe uma prova que certifica um resultado, então este resultado é válido. O seguinte corolário (bem natural) mostra que todo teorema é válido:

COROLÁRIO III.2.4. Dada uma sentença φ de $\mathrm{L_I}$, se $\vdash \varphi$, então $\models \varphi$. Em particular, a sentença $\bot$ não é um teorema.

Demonstração. Se $\vdash \varphi$, então para todas M e $\tau : \mathrm{Par}(\Delta) \longrightarrow 2^{\mathrm{E(M)}}$ vale $\mathrm{M}[\top] \leq \mathrm{M}[\varphi]$, e portanto, $\mathrm{M}[\varphi] = 1$. Em particular, vemos que $\bot$ não é um teorema. ⊣

[g] Seguindo a distinção entre linguagem objeto e metalinguagem, o resultado chamado de Teorema III.2.3 é um metateorema, uma vez que ele é um teorema sobre teoremas.

EXEMPLO III.2.5 (Motivação das Restrições em Regras). Algumas regras de dedução e reescrita apresentam restrições que são compatíveis com a definição de verdade para sentenças. Vejamos alguns exemplos:

(1) Uma sentença da forma $\exists x\varphi(x) \to \forall x\varphi(x)$ não é um teorema. De fato, tomemos M tal que $\mathrm{E}(\mathrm{M}) = \{\,0\,\}$ e $\mathcal{I}(\mathrm{M}) = \{\,\emptyset\,\}$. Neste caso, vemos que $\mathrm{M} \models \exists x\,\mathrm{Ind}\,x$ e $\mathrm{M} \not\models \forall x\,\mathrm{Ind}\,x$. Isso mostra a importância da restrição feita na regra $\exists^{\bullet}_{\mathrm{E}}$. Portanto, uma regra $\exists^{*}_{\mathrm{E}}$ que permita a construção de árvores da forma

$$\left.\begin{array}{l} \vdots \\ \dfrac{\frac{y}{x}\varphi(x) \Rightarrow \frac{y}{x}\varphi(x)}{\exists x\varphi(x) \Rightarrow \frac{y}{x}\varphi(x)}\ \exists^{*}_{\mathrm{E}} \\ \dfrac{\exists x\varphi(x) \Rightarrow \frac{y}{x}\varphi(x)}{\exists x\varphi(x) \Rightarrow \forall x\varphi(x)}\ \forall^{\bullet}_{\mathrm{D}} \\ \dfrac{\exists x\varphi(x) \Rightarrow \forall x\varphi(x)}{\Rightarrow \exists x\varphi(x) \to \forall x\varphi(x)}\ \to_{\mathrm{D}} \end{array}\right\} \text{não é uma prova}$$

não é compatível com a noção semântica apresentada. Raciocínio análogo para a restrição da regra $\forall^{\bullet}_{\mathrm{D}}$.

(2) Uma sentença da forma $\forall x(\psi(x) \vee \phi(x)) \to (\forall x\psi(x) \vee \forall x\phi(x))$ não é um teorema. De fato, tomemos M tal que $\mathrm{E}(\mathrm{M}) = \{\,0, 1\,\}$ e $\mathcal{I}(\mathrm{M}) = 2^{\mathrm{E}(\mathrm{M})} - \{\,\{\,0\,\}\,\}$. Nesse caso vemos que $\mathrm{M} \models \forall x(\mathrm{Ind}\,x \vee \mathrm{Sng}\,x)$ e $\mathrm{M} \not\models \forall x\,\mathrm{Ind}\,x \vee \forall x\,\mathrm{Sng}\,x$. Isso mostra a importância da restrição feita nas operações prenex. ⊣

Suponhamos que T seja um conjunto cujos elementos são todos sentenças de $\mathrm{L_I}$. Dizemos que uma sentença φ de $\mathrm{L_I}$ é um *teorema de* T e escrevemos $\mathrm{T} \vdash \varphi$ quando existem um multiconjunto finito Γ de sentenças de T e uma prova do sequente $\Gamma \Rightarrow \varphi$. Dizemos que T é uma *teoria* quando, para toda sentença φ de $\mathrm{L_I}$, a condição $\mathrm{T} \vdash \varphi$ é suficiente para que φ pertença ao conjunto T. Dizemos que uma teoria T é *finitamente axiomatizável* quando existe um conjunto finito U de sentenças de $\mathrm{L_I}$ tais que toda sentença de T é um teorema de U. Neste caso, dizemos também que as sentenças de U são *axiomas da teoria* T ou que T é o *fecho por consequências lógicas* de U. Dada uma estrutura M para a linguagem $\mathrm{L_I}$ e um conjunto de sentenças T, escrevemos $\mathrm{M} \models \mathrm{T}$ para indicar que $\mathrm{M} \models \varphi$ para toda sentença φ de T. Neste caso, dizemos também que M é um *modelo* de T. Dizemos que T *acarreta* uma sentença φ e escrevemos $\mathrm{T} \models \varphi$ quando todo modelo de T é um modelo de φ.

COROLÁRIO III.2.6. Dados uma sentença φ e um subconjunto T de sentenças de $\mathrm{L_I}$, se $\mathrm{T} \vdash \varphi$, então $\mathrm{T} \models \varphi$.

Demonstração. Se $\mathrm{T} \vdash \varphi$, então existem um multiconjunto finito Γ de sentenças de T e uma prova do sequente $\Gamma \Rightarrow \varphi$. Do Teorema III.2.3, vemos que para toda M vale $\mathrm{M}[\wedge\Gamma] \leq \mathrm{M}[\varphi]$. Se M é tal que $\mathrm{M} \models \mathrm{T}$, então $\mathrm{M}[\wedge\Gamma] = 1$, e portanto, $\mathrm{M}[\varphi] = 1$. Concluímos assim que $\mathrm{T} \models \varphi$. ⊣

Uma teoria T é *inconsistente* quando $\bot \in \mathrm{T}$. Uma teoria que não é inconsistente é chamada de teoria *consistente*. Estamos interessados em teorias consistentes. Fe-

lizmente o Teorema III.2.3 fornece condições suficientes[h] para que uma teoria seja consistente e este é o resultado do seguinte corolário.

COROLÁRIO III.2.7. Dado um subconjunto T de sentenças de L_I, se T tem um modelo, então T é consistente.

Demonstração. A prova é indireta e é feita por meio da contrapositiva. Se $\bot \in T$, então segue do Corolário III.2.6 que $T \models \bot$. Como $M[\bot] = 0$ para toda estrutura M, vemos que T não tem modelo. ⊣

A teoria de matroides na linguagem L_I é o fecho por consequências lógicas do conjunto T_I cujos elementos são as sentenças

$$\exists x \operatorname{Ind} x$$
$$\forall x \forall y \operatorname{Her} xy$$
$$\forall x \forall y \operatorname{Exc} xy$$

obtidas das fórmulas apresentadas no Exemplo III.2.2. Uma matroide é um modelo de T_I e a classe destes modelos será denotada por $\operatorname{Mod}(T_I)$. Dizemos que $M, N \in \operatorname{Mod}(T_I)$ são *elementarmente equivalentes* e escrevemos $M \equiv N$ quando para toda sentença φ de L_I, vale $M[\varphi] = N[\varphi]$. Observemos que se $M \cong N$, então $M \equiv N$. Escrevamos $T_I + \varphi$ para indicar o conjunto de axiomas obtidos de T_I pela adição da sentença φ e denotemos por $\operatorname{Mod}(T_I + \varphi)$ a classe dos modelos $M \in \operatorname{Mod}(T_I)$ tais que $M \models \varphi$. Como as estruturas estudadas são finitas, obtemos o resultado da Proposição III.2.8 de maneira bem natural como é feito por L. Libkin no Lema 3.4 [10] para outros tipos de estruturas finitas.

PROPOSIÇÃO III.2.8. Dada $M \in \operatorname{Mod}(T_I)$, existe uma sentença θ_M de L_I tal que para toda $N \in \operatorname{Mod}(T_I)$ vale $M \cong N$ sse $N \in \operatorname{Mod}(T_I + \theta_M)$.

A Proposição III.2.8 mostra que a teoria de matroides isomorfas à uma matroide fixa é axiomatizável, o que evidencia que a noção de equivalência elementar não é interessante para resolver problemas de indefinibilidade neste contexto monádico de segunda ordem. Por outro lado, a existência da sentença θ_M que caracteriza a matroide M (a menos de isomorfismo) motiva a seguinte pergunta: é possível fornecer condições semânticas necessárias e suficientes para concluir que uma matroide é isomorfa a um menor de outra? A resposta é positiva, como mostra a Proposição III.2.9, que é uma adaptação para a presente linguagem do Lema 5.1 provado por P. Hliněný [6].

PROPOSIÇÃO III.2.9. Dada $N \in \operatorname{Mod}(T_I)$, existe uma sentença μ_N de L_I tal que para toda $M \in \operatorname{Mod}(T_I)$ vale $N \preceq M$ sse $M \models \mu_N$.

Demonstração. Suponhamos que $N \preceq M$. Neste caso, existem $X, Y \subseteq E(M)$ disjuntos tais que $N \cong M \setminus X / Y$. Se Y_1 é uma base de $M \mid Y$ e X_1 é uma base de $M^* \mid X$, então segue do Teorema II.3.10 que

$$M \setminus X / Y = M \setminus [X_1 \cup (Y - Y_1)] / [Y_1 \cup (X - X_1)]$$

[h] As pessoas familiarizadas com lógicas podem se perguntar: o sistema de dedução apresentado é completo? A resposta é negativa, uma vez que o Teorema da Compacidade falha neste contexto: lidamos apenas com estruturas finitas para interpretar a linguagem objeto (vide L. Libkin [10]).

com $X_1 \cup (Y - Y_1) \in \mathcal{I}(M^*)$ e $Y_1 \cup (X - X_1) \in \mathcal{I}(M)$. Escrevendo $I^* = X_1 \cup (Y - Y_1)$ e $I = Y_1 \cup (X - X_1)$, obtemos um isomorfismo $\varphi : E(N) \longrightarrow E(M \setminus I^* / I)$ de N em $M \setminus I^* / I$. Da Proposição II.3.11, sabemos que um conjunto $D_1 \subseteq E(N)$ é dependente em $M \setminus I^* / I$ sse existe $D_2 \subseteq E(M)$ dependente em M tal que $D_2 - \varphi(D_1) \subseteq I$. Como N é finita, podemos supor que $|E(N)| = m$. Tomemos $k = 2^m$ e enumeremos os nomes dos elementos de $2^{E(N)}$ na forma $c_1, \ldots, c_k$. Para cada c_n, definamos a fórmula:

$$\psi_n(c_n, x) = \exists x_n \forall y_n (\neg \operatorname{Ind} x_n \wedge \operatorname{Sng} y_n \wedge (\neg y_n \sqsubseteq x_n \vee y_n \sqsubseteq x \vee y_n \sqsubseteq c_n)).$$

Nas fórmulas $\psi_1(c_1, x), \ldots, \psi_k(c_k, x)$ a variável livre x desempenha o papel do conjunto $I \subseteq E(M)$ que é contraído em M. Dado $t \in \{0, 1\}$, definamos N_t o conjunto dos $n \in \mathbb{N}$ com $1 \leq n \leq k$ tais que $N[\operatorname{Ind} c_n] = t$. Por fim, basta definir:

$$\mu_N = \exists z_1 \cdots \exists z_k \exists z_{k+1} \left(\bigwedge_{n \in N_0} \psi_n(z_n, z_{k+1}) \wedge \bigwedge_{n \in N_1} \neg \psi_n(z_n, z_{k+1}) \right). \qquad \dashv$$

III.3 INDEFINIBILIDADE: PRIMEIRA PARTE

Apresentaremos nesta e nas demais seções seguintes os resultados lógicos principais deste trabalho. Serão apresentados primeiro os resultados sobre indefinibilidade da representabilidade linear que decorrem do Teorema III.3.7. As referências principais desta seção são J. Oxley [15] e D. Mayhew, M. Newman e G. Whittle [12].

Uma classe $K \subseteq \operatorname{Mod}(T_I)$ é *definível* quando existe um conjunto finito U de sentenças de L_I tal que $M \models U$ sse $M \in K$. Quando K é definível e U é o conjunto de sentenças que a define, escrevemos $K = \operatorname{Mod}(T_I + U)$.

EXEMPLO III.3.1 (Definibilidade).

(1) Uma matroide $U \in \operatorname{Mod}(T_I)$ é uniforme sse todo conjunto dependente de U contém uma base de U. Isto mostra que a classe das matroides uniformes é $\operatorname{Mod}(T_I + \upsilon)$, onde

$$\upsilon = \forall x \exists y (\neg \operatorname{Ind} x \rightarrow \operatorname{Base} y \wedge y \sqsubseteq x).$$

(2) Suponhamos que S seja um conjunto finito de matroides. Segue da Proposição III.2.9 que existe a conjunção $\varphi_S \in \operatorname{Snt}(L_I)$ das sentenças $\neg \mu_N$ para cada $N \in S$. Isto permite definir a classe $\operatorname{Mod}(T_I + \varphi_S)$ das matroides que não possuem menores isomorfos às matroides do conjunto S. Isto mostra que se a Conjectura de Rota[i] for verdadeira, então a classe das matroides linearmente representáveis sobre um corpo finito fixo é definível [12]. $\dashv\!\dashv$

Um tipo interessante de problemas é o seguinte: dada uma propriedade P pertinente às matroides é possível obter um conjunto finito de sentenças de L_I que define a classe das matroides que possuem a propriedade P? Em particular, estudaremos o Problema III.3.2. A Proposição III.2.8 elimina toda esperança de

[i] Uma matroide que é uma obstrução minimal para a representabilidade linear sobre um corpo é chamada de menor excluído para tal representabilidade. A Conjectura de Rota é a seguinte: o número de menores excluídos da representabilidade linear sobre um corpo de q elementos é finito. Vide G. Gordon e J. McNulty [3] para uma discussão mais detalhada sobre esta conjectura.

utilizar a noção de equivalência elementar de modelos para resolver o problema apresentado. Por outro lado, podemos procurar por alguma restrição natural de tal noção de equivalência exigindo algum tipo de modificação sobre as sentenças e estruturas analisadas.

PROBLEMA III.3.2. A classe das matroides linearmente representáveis é definível?

Suponhamos que M e N sejam matroides tais que $E(M) \cap E(N) = \emptyset$. A *soma direta* de M e N é a matroide $M \oplus N$ sobre $E(M) \cup E(N)$ tal que $I \in \mathcal{I}(M \oplus N)$ sse $I \cap E(M) \in \mathcal{I}(M)$ e $I \cap E(N) \in \mathcal{I}(N)$. Observemos que

$$r_{M\oplus N}(X) = r_M(X \cap E(M)) + r_N(X \cap E(N))$$

para todo $X \subseteq E(M) \cup E(N)$. Dadas M, N, $U \in \mathrm{Mod}(T_I)$, dizemos que U é *compatível* com (M, N) quando $E(U) \cap [E(M) \cup E(N)] = \emptyset$. Suponhamos que m seja um número natural positivo. Um *m-certificado* para (M, N) é um par $(U, \varphi) \in \mathrm{Mod}(T_I) \times \mathrm{Snt}(L_I)$ no qual φ é uma sentença de L_I com exatamente m variáveis e U é uma matroide compatível com (M, N) tal que

$$(U \oplus M)[\varphi] + (U \oplus N)[\varphi] = 1.$$

Isso permite definir em $\mathrm{Mod}(T_I)$ uma relação diádica pondo $M \#_m N$ sse existe um m-certificado para (M, N). A seguinte proposição mostra que a relação $\#_m$ é uma *relação de apartness*[j].

PROPOSIÇÃO III.3.3. A relação $\#_m$ é uma relação de apartness em $\mathrm{Mod}(T_I)$.

Demonstração. Vamos provar que a relação $\#_m$ satisfaz o seguinte: se $M \#_m N$, então $M \#_m L$ ou $N \#_m L$. Suponhamos que $M \#_m N$. Neste caso, existe um m-certificado (U, φ) para (M, N). Disto, vemos que $(U \oplus M)[\varphi] + (U \oplus N)[\varphi] = 1$. Dada L em $\mathrm{Mod}(T_I)$, se não existe um m-certificado para (L, M), então $(U \oplus L)[\varphi] = (U \oplus M)[\varphi]$, e assim, (U, φ) é um m-certificado para (L, N). De maneira análoga, se não existe um m-certificado para (L, N), então $(U \oplus L)[\varphi] = (U \oplus N)[\varphi]$, e assim, (U, φ) é um m-certificado para (L, M). Isto mostra que existe um m-certificado para (L, M) ou existe um m-certificado para (L, N), e portanto, $M \#_m L$ ou $N \#_m L$. As demais propriedades de $\#_m$ são de verificação rotineira. ⊣

O complemento de uma relação de apartness é uma relação de equivalência e a verificação disto é relativamente simples (vide A. S. Troelstra e H. Schwichtenberg [19]). Dizemos que M e N são *m-equivalentes* e escrevemos $M \equiv_m N$ quando não é o caso que $M \#_m N$. Em outras palavras, M e N são m-equivalentes quando $U \oplus M$ e $U \oplus N$ não podem ser distinguidas por sentenças de L_I com exatamente m variáveis, qualquer que seja a matroide U compatível com (M, N). Neste caso, se $(U, \varphi) \in \mathrm{Mod}(T_I) \times \mathrm{Snt}(L_I)$ é um par no qual φ é uma sentença de L_I com exatamente m variáveis e U é uma matroide compatível com (M, N), então

$$(U \oplus M)[\varphi] = (U \oplus N)[\varphi].$$

A relação de m-equivalência utiliza a noção de verdade de sentenças em sua definição. Isto motiva a busca por alguma forma de relacionar a verdade de

[j] Uma relação diádica # é uma relação de apartness sse satisfaz (i) não é o caso que $a \# a$, (ii) se $a \# b$, então $b \# a$ e (iii) se $a \# b$, então $a \# c$ ou $b \# c$. Vide A. S. Troelstra e H. Schwichtenberg [19] para uma discussão mais detalhada deste tipo de relação.

uma sentença de m variáveis com algum tipo de objeto que contenha as informações locais relevantes e necessárias sobre a matroide analisada. Escrevamos $\Sigma = \{0, 1, 2\}$. Para cada número natural positivo m, um *m-registro* é uma função $\mathrm{R} : \{1, \ldots, m+2\} \times \{1, \ldots, m\} \longrightarrow \Sigma$ tal que a imagem direta de elementos de $\{1, \ldots, m\} \times \{1, \ldots, m\}$ é ou 0 ou 1 e a imagem direta de elementos de $\{m+2\} \times \{1, \ldots, m\}$ é ou 0 ou 1 ou 2. Podemos representar um m-registro utilizando um quadro como mostra a Figura III.3.1, no qual rotulamos as colunas e linhas de acordo com o que mostra a mesma figura. O número máximo possível de m-registros é $2^{m(m+1)} \cdot 3^m$. Suponhamos que φ seja uma fórmula de $\mathrm{L_I}$ livre de quantificadores e cujas variáveis sejam x_1, ..., x_m. Dados dois m-registros R e S, definimos a relação $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\,\varphi)$ de *φ-compatibilidade de m-registros* recursivamente da seguinte forma:

(1) $\mathrm{R} \not\equiv \mathrm{S}\ (\mathrm{comp}\,\bot)$

(2) $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\,\mathrm{Ind}\,x_n)$ sse $\mathrm{R}(m+1, n) \cdot \mathrm{S}(m+1, n) = 1$.

(3) $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\,\mathrm{Sng}\,x_n)$ sse $\mathrm{R}(m+2, n) + \mathrm{S}(m+2, n) = 1$, onde $n \in \{1, \ldots, m\}$.

(4) $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\,x_i \sqsubseteq x_j)$ sse $\mathrm{R}(i, j) \cdot \mathrm{S}(i, j) = 1$, onde $i, j \in \{1, \ldots, m\}$.

(5) $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\,\alpha \wedge \beta)$ sse $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\,\alpha)$ e $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\,\beta)$.

(6) $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\,\alpha \vee \beta)$ sse $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\,\alpha)$ ou $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\,\beta)$.

(7) $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\,\alpha \rightarrow \beta)$ sse $\mathrm{R} \not\equiv \mathrm{S}\ (\mathrm{comp}\,\alpha)$ ou $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\,\beta)$.

A noção de registro apresentada é muito geral e isso motiva a busca por uma definição de algum tipo de registro que lide com alguma escolha particular de matroide e de conjuntos desta matroide. Uma *matroide empilhada* é uma lista $(\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m)$, na qual $\mathrm{M} \in \mathrm{Mod}(\mathrm{T_I})$ e X_1, ..., $\mathrm{X}_m \subseteq \mathrm{E}(\mathrm{M})$. Podemos construir m-registros associados a uma matroide empilhada $(\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m)$ que codificam as informações básicas relevantes para a linguagem $\mathrm{L_I}$ sobre os conjuntos X_1, ..., X_m. Para cada matroide empilhada $(\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m)$, definamos o m-registro $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!]$ recursivamente da seguinte maneira:

(1) Para $i, j \in \{1, \ldots, m\}$, definimos $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!](i, j) = 1$ sse $\mathrm{X}_i \subseteq \mathrm{X}_j$.

(2) Para $n \in \{1, \ldots, m\}$, definimos $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!](m+1, n) = 1$ sse $\mathrm{X}_n \in \mathcal{I}(\mathrm{M})$.

(3) Para $n \in \{1, \ldots, m\}$, definimos:

(3.1) $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!](m+2, n) = 0$ sse $\mathrm{X}_n = \emptyset$.

(3.2) $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!](m+2, n) = 1$ sse $|\mathrm{X}_n| = 1$.

(3.3) $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!](m+2, n) = 2$ sse $1 < |\mathrm{X}_n|$.

Utilizando a noção de compatibilidade de m-registros e os m-registros construídos usando matroides empilhadas é possível alcançar o objetivo de relacionar satisfabilidade de instâncias de fórmulas com compatibilidade de registros, pelo menos para fórmulas livres de quantificadores neste primeiro momento. Este é o conteúdo do lema a seguir:

	x_1	x_2	$\cdots$	x_m
x_1	$[\![\mathrm{M}, -]\!](1,1)$	$[\![\mathrm{M}, -]\!](1,2)$	$\cdots$	$[\![\mathrm{M}, -]\!](1,m)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_m	$[\![\mathrm{M}, -]\!](m,1)$	$[\![\mathrm{M}, -]\!](m,2)$	$\cdots$	$[\![\mathrm{M}, -]\!](m,m)$
Ind	$[\![\mathrm{M}, -]\!](m+1,1)$	$[\![\mathrm{M}, -]\!](m+1,2)$	$\cdots$	$[\![\mathrm{M}, -]\!](m+1,m)$
Sng	$[\![\mathrm{M}, -]\!](m+2,1)$	$[\![\mathrm{M}, -]\!](m+2,2)$	$\cdots$	$[\![\mathrm{M}, -]\!](m+2,m)$

Figura III.3.1: A figura ilustra um m-registro genérico associado à uma matroide empilhada.

LEMA III.3.4. [12, Afirmação 3.1.1] Suponhamos que φ seja uma fórmula de $\mathrm{L_I}$ livre de quantificadores e cujas variáveis sejam x_1, ..., x_m. Tomemos M, N $\in$ $\mathrm{Mod(T_I)}$ tais que $\mathrm{E(M)} \cap \mathrm{E(N)} = \emptyset$ e tomemos também $\mathrm{X_1}$, ..., $\mathrm{X}_m \subseteq \mathrm{E(M)}$ e $\mathrm{Y_1}$, ..., $\mathrm{Y}_m \subseteq \mathrm{E(N)}$. Para cada $i \in \{1, \ldots, m\}$, denotemos por c_i o nome de $\mathrm{X}_i \cup \mathrm{Y}_i$ em $\mathrm{L_I(M \oplus N)}$. As seguintes afirmações são equivalentes:

(1) $[\![\mathrm{M}, \mathrm{X_1}, \ldots, \mathrm{X}_m]\!] \equiv [\![\mathrm{N}, \mathrm{Y_1}, \ldots, \mathrm{Y}_m]\!]$ (comp φ).

(2) $\mathrm{M} \oplus \mathrm{N} \models \frac{c_1,\ldots,c_m}{x_1,\ldots,x_m}\varphi$.

Demonstração. Escrevamos $\mathrm{R} = [\![\mathrm{M}, \mathrm{X_1}, \ldots, \mathrm{X}_m]\!]$ e $\mathrm{S} = [\![\mathrm{N}, \mathrm{Y_1}, \ldots, \mathrm{Y}_m]\!]$. Primeiro, vamos mostrar que o resultado é válido para fórmulas atômicas:

(1) Temos $\mathrm{M} \oplus \mathrm{N} \models \frac{c_1,\ldots,c_m}{x_1,\ldots,x_m} \mathrm{Ind}\, x_n$ sse $\mathrm{M} \oplus \mathrm{N} \models \mathrm{Ind}\, c_n$ sse $\mathrm{X}_n \cup \mathrm{Y}_n \in \mathcal{I}(\mathrm{M} \oplus \mathrm{N})$ sse $\mathrm{X}_n \mathcal{I}(\mathrm{M})$ e $\mathrm{Y}_n \mathcal{I}(\mathrm{N})$ sse $\mathrm{R}(m+1, n) = 1$ e $\mathrm{S}(m+1, n) = 1$ sse $\mathrm{R}(m+1, n) \cdot \mathrm{S}(m+1, n) = 1$ sse $\mathrm{R} \equiv \mathrm{S}$ (comp $\mathrm{Ind}\, x_n$).

(2) Temos $\mathrm{M} \oplus \mathrm{N} \models \frac{c_1,\ldots,c_m}{x_1,\ldots,x_m} \mathrm{Sng}\, x_n$ sse $\mathrm{M} \oplus \mathrm{N} \models \mathrm{Sng}\, c_n$ sse $|\mathrm{X}_n \cup \mathrm{Y}_n| = 1$ sse $|\mathrm{X}_n| + |\mathrm{X}_n| = 1$ sse $\mathrm{R}(m+1, n) + \mathrm{S}(m+1, n) = 1$ sse $\mathrm{R} \equiv \mathrm{S}$ (comp $\mathrm{Sng}\, x_n$).

(3) Temos $\mathrm{M} \oplus \mathrm{N} \models \frac{c_1,\ldots,c_m}{x_1,\ldots,x_m} x_i \sqsubseteq x_j$ sse $\mathrm{M} \oplus \mathrm{N} \models \mathrm{Sng}\, c_i \sqsubseteq c_j$ sse $\mathrm{X}_i \cup \mathrm{Y}_i \subseteq \mathrm{X}_j \cup \mathrm{Y}_j$ sse $\mathrm{X}_i \subseteq \mathrm{X}_j$ e $\mathrm{Y}_i \subseteq \mathrm{Y}_j$ sse $\mathrm{R}(i, j) \cdot \mathrm{S}(i, j) = 1$ sse $\mathrm{R} \equiv \mathrm{S}$ (comp $x_i \sqsubseteq x_j$).

Dada uma fórmula φ de $\mathrm{L_I}$ livre de quantificadores, suponhamos que o resultado seja válido para toda fórmula de $\mathrm{L_I}$ com comprimento menor que o de φ e livre de quantificadores. A seguir, analisaremos os casos em que φ é da forma $\alpha \square \beta$ e usar a hipótese de indução. Vamos omitir a expressão $\frac{c_1,\ldots,c_m}{x_1,\ldots,x_m}$.

(4) $\mathrm{M} \oplus \mathrm{N} \models \alpha \wedge \beta$ sse $\mathrm{M} \oplus \mathrm{N} \models \alpha$ e $\mathrm{M} \oplus \mathrm{N} \models \beta$ sse $\mathrm{R} \equiv \mathrm{S}$ (comp α) e $\mathrm{R} \equiv \mathrm{S}$ (comp β) sse $\mathrm{R} \equiv \mathrm{S}$ (comp $\alpha \wedge \beta$).

(5) $M \oplus N \models \alpha \vee \beta$ sse $M \oplus N \models \alpha$ ou
$M \oplus N \models \beta$
sse $R \equiv S\ (\mathrm{comp}\,\alpha)$ ou
$R \equiv S\ (\mathrm{comp}\,\beta)$
sse $R \equiv S\ (\mathrm{comp}\,\alpha \vee \beta)$.

(6) $M \oplus N \models \alpha \to \beta$ sse $M \oplus N \not\models \alpha$ ou
$M \oplus N \models \beta$
sse $R \not\equiv S\ (\mathrm{comp}\,\alpha)$ ou
$R \equiv S\ (\mathrm{comp}\,\beta)$
sse $R \equiv S\ (\mathrm{comp}\,\alpha \to \beta)$.

O resultado segue do Princípio de Indução. ⊣

Agora, vamos seguir com o estudo sistemático para estender a noção de compatibilidade para sentenças. Neste caso, vamos ter que dar conta de explicar como funciona a compatibilidade quando ocorrem quantificadores em uma fórmula. Para isto, vamos apresentar uma noção de árvore e o Corolário III.1.13 desempenhará um papel muito importante em nossas análises. Uma 0-*árvore* é um registro e para cada $m \in \mathbb{N}$, uma $(m+1)$-*árvore* é um conjunto não-vazio de m-árvores. Sabemos que o número de 0-árvores é no máximo $2^{m(m+1)} \cdot 3^m$. Definamos $\sigma_m : \mathbb{N} \longrightarrow \mathbb{N}$ pondo $\sigma_m(0) = 2^{m(m+1)} \cdot 3^m$ e $\sigma_m(n+1) = 2^{\sigma_m(n)}$. Em virtude da Proposição III.3.5, vemos que o número de m-árvores é no máximo o número $\sigma_m(m)$. O resultado desta proposição pode ser provado por indução.

PROPOSIÇÃO III.3.5. O número de m-árvores é no máximo $\sigma_m(m)$[k].

Em virtude do Corolário III.1.13 e do Corolário III.2.4, podemos definir a compatibilidade de árvores para o caso em que as fórmulas estão em forma normal prenex. Dada uma fórmula φ de L_I em forma normal prenex com m variáveis livres $x_1, \ldots, x_m$ e n variáveis ligadas $x_{m+1}, \ldots, x_{m+n}$ e duas n-árvores T_n e T'_n, definimos a relação $T_n \equiv T'_n\ (\mathrm{comp}\,\varphi)$ de φ-*compatibilidade de n-árvores* recursivamente da seguinte forma:

(1) Suponhamos que $n = 0$. Neste caso, temos dois registros e a φ-compatibilidade de registros já foi definida.

(2) Dado $k \in \{0, \ldots, n-1\}$, suponhamos que para toda fórmula ψ de L_I em forma normal prenex com número de variáveis ligadas $s \leq k$ a ψ-compatibilidade de s-árvores esteja definida. Dada uma fórmula φ de L_I em forma normal prenex com m variáveis livres $x_1, \ldots, x_m$ e $k+1$ variáveis ligadas $x_{m+1}, \ldots, x_{m+k+1}$, suponhamos que

$$\varphi = Q_{k+1}x_{m+k+1} \cdots Q_1 x_{m+1}\,\psi,$$

de modo que ψ seja livre de quantificadores. Definamos

$$\alpha = Q_k x_{m+k} \cdots Q_1 x_{m+1}\,\psi.$$

Tomemos $(k+1)$-árvores T_{k+1} e T'_{k+1} quaisquer. Temos dois casos para analisar:

[k] A noção de m-equivalência diz respeito à inexistência de certos tipos de testemunhas que são compostas por sentenças com m variáveis. Usando esta motivação, podemos identificar este m na expressão "m-árvore" na proposição com o número de variáveis da sentença candidata à sentença de uma testemunha.

(1) O primeiro caso é $Q_{k+1} = \exists$. Definimos $T_{k+1} \equiv T'_{k+1}$ (comp φ) sse existem $T_k \in T_{k+1}$ e $T'_k \in T'_{k+1}$ tais que $T_k \equiv T'_k$ (comp α).

(2) O segundo caso é $Q_{k+1} = \forall$. Definimos $T_{k+1} \equiv T'_{k+1}$ (comp φ) sse para todas $T_k \in T_{k+1}$ e $T'_k \in T'_{k+1}$ temos $T_k \equiv T'_k$ (comp α).

A noção de árvore apresentada é muito geral e isso motiva a busca por uma definição de algum tipo de árvore que lide com alguma escolha particular de matroide e de conjuntos desta matroide. Consideremos $M \in \mathrm{Mod}(T_I)$ e um número natural positivo m. Pensando na relação de m-equivalência, o papel desempenhado por este m é o do número de variáveis de uma sentença que faz parte de um m-certificado. Tomemos $X_1, \ldots, X_k \subseteq E(M)$ para algum $k \leq m$ e formemos a matroide empilhada $(M, X_1, \ldots, X_k)$. O papel desempenhado por este k é o do número de variáveis livres de uma fórmula. Escrevamos $n = m - k$. O papel desempenhado por este n é o do número de variáveis ligadas de uma fórmula. A n-árvore $[\![M, X_1, \ldots, X_k]\!]_n$ associada à matroide empilhada $(M, X_1, \ldots, X_k)$ é definida recursivamente da seguinte maneira [12]:

(1) Suponhamos que $n = 0$. Neste caso definimos

$$[\![M, X_1, \ldots, X_k]\!]_0 = [\![M, X_1, \ldots, X_m]\!].$$

(2) Dado $n \in \{0, \ldots, m-1\}$, suponhamos que $(M, X_1, \ldots, X_k)$ seja tal que $k = m-(n+1)$ e suponhamos também que $[\![M, Y_1, \ldots, Y_j]\!]_n$ esteja definida sempre que $m-j \leq n$. Dado $X \subseteq E(M)$, tomemos a matroide empilhada $(M, X_1, \ldots, X_k, X_{k+1})$. O comprimento da lista $X_1, \ldots, X_k, X_{k+1}$ é $k+1$. De $n = m-k$, vemos que $n-1 = m-(k+1)$, e assim, $m-(k+1) \leq n$. Do passo de indução, vemos que está definida a n-árvore $[\![M, X_1, \ldots, X_k, X_{k+1}]\!]_n$. Definamos então a $(n+1)$-árvore

$$[\![M, X_1, \ldots, X_k]\!]_{n+1} = \left\{ [\![M, X_1, \ldots, X_k, X_{k+1}]\!]_n : X_{k+1} \subseteq E(M) \right\}.$$

Façamos uma pequena reflexão sobre as construções recursivas de n-árvores associadas às escolhas de matroides empilhadas $(M, X_1, \ldots, X_k)$. Partindo da motivação de m e k como os números totais de variáveis e de variáveis livres de uma fórmula em forma normal prenex, vemos que o processo de construção reflete os princípios que usamos para definir a noção de compatibilidade de n-árvores para $n = m - k$. Ao construir a $n+1$ árvore $[\![M, X_1, \ldots, X_k]\!]_{n+1}$, consideramos todas as n-árvores $[\![M, X_1, \ldots, X_k, X_{k+1}]\!]_n$, onde tomamos $X_{k+1} \subseteq E(M)$. Observemos que o processo de aumentar a lista $X_1, \ldots, X_k$ para $X_1, \ldots, X_k, X_{k+1}$ corresponde ao processo de remover o quantificador mais à esquerda no prefixo da fórmula em forma normal prenex. Assim, podemos analisar a compatibilidade de n-árvores de maneira bem natural. O seguinte Lema III.3.6 mostra que a decisão de compatibilidade de árvores é equivalente à satisfabilidade de fórmulas por somas diretas. Em virtude da existência da forma normal prenex na linguagem objeto que estamos estudando, o seguinte lema é uma generalização natural do Lema III.3.4.

LEMA III.3.6. [12, Afirmação 3.1.1] Tomemos uma fórmula φ de L_I em forma normal prenex na qual ocorrem m variáveis livres $x_1, \ldots, x_m$ e n variáveis ligadas $x_{m+1}, \ldots, x_{m+n}$, tomemos $M, N \in \mathrm{Mod}(T_I)$ tais que $E(M) \cap E(N) = \emptyset$ e tomemos também $X_1, \ldots, X_m \subseteq E(M)$ e $Y_1, \ldots, Y_m \subseteq E(N)$. Para cada $i \in \{1, \ldots, m\}$, denotemos por c_i o nome de $X_i \cup Y_i$ em $L_I(M \oplus N)$. As seguintes afirmações são equivalentes:

(1) $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!]_n \equiv [\![\mathrm{N}, \mathrm{Y}_1, \ldots, \mathrm{Y}_m]\!]_n$ (comp φ).

(2) $\mathrm{M} \oplus \mathrm{N} \models \frac{c_1,\ldots,c_m}{x_1,\ldots,x_m}\varphi$.

Demonstração. A prova é feita por indução no número n de variáveis ligadas da fórmula em forma normal prenex. O caso $n = 0$ é válido pelo Lema III.3.4. Suponhamos que para toda fórmula em forma normal prenex ψ de $\mathrm{L_I}$ de n variáveis ligadas e m variáveis livres a afirmação seja verdadeira. Dada uma fórmula em forma normal prenex φ de $\mathrm{L_I}$ com m variáveis livres x_1, ..., x_m e $n+1$ variáveis ligadas x_{m+1}, ..., x_{m+n+1}, suponhamos que

$$\varphi = \mathrm{Q}_{n+1}x_{m+n+1} \cdots \mathrm{Q}_1 x_{m+1}\psi,$$

de modo que ψ seja livre de quantificadores. Definamos

$$\alpha = \mathrm{Q}_n x_{m+n} \cdots \mathrm{Q}_1 x_{m+1}\psi.$$

Dados X_1, ..., $\mathrm{X}_m \subseteq \mathrm{E(M)}$ e Y_1, ..., $\mathrm{Y}_m \subseteq \mathrm{E(N)}$, tomemos as $(n+1)$-árvores $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!]_{n+1}$ e $[\![\mathrm{N}, \mathrm{Y}_1, \ldots, \mathrm{Y}_m]\!]_{n+1}$. Temos dois casos para analisar:

(1) Suponhamos que $\mathrm{Q}_{n+1} = \exists$. Temos

$$[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!]_{n+1} \equiv [\![\mathrm{N}, \mathrm{Y}_1, \ldots, \mathrm{Y}_m]\!]_{n+1} \text{ (comp } \varphi)$$

sse existem árvores $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m, \mathrm{X}_{n+1}]\!]_n \in [\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!]_{n+1}$ e $[\![\mathrm{N}, \mathrm{Y}_1, \ldots, \mathrm{Y}_m, \mathrm{Y}_{n+1}]\!]_n \in [\![\mathrm{N}, \mathrm{Y}_1, \ldots, \mathrm{Y}_m]\!]_{n+1}$ tais que

$$[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m, \mathrm{X}_{n+1}]\!]_n \equiv [\![\mathrm{N}, \mathrm{Y}_1, \ldots, \mathrm{Y}_m, \mathrm{Y}_{n+1}]\!]_n \text{ (comp } \alpha).$$

Da hipótese de indução, isto é equivalente a $\mathrm{M} \oplus_{\mathrm{L}} \mathrm{N} \models \frac{c_1,\ldots,c_m,c_{n+1}}{x_1,\ldots,x_m,x_{m+n+1}}\alpha$, onde c_{n+1} é o nome de $\mathrm{X}_{n+1} \cup \mathrm{Y}_{n+1}$ em $\mathrm{L_I(M \oplus N)}$. Da Proposição III.2.1, isto é equivalente a $\mathrm{M} \oplus_{\mathrm{L}} \mathrm{N} \models \frac{c_1,\ldots,c_m}{x_1,\ldots,x_m}\varphi$.

(2) Suponhamos que $\mathrm{Q}_{n+1} = \forall$. Temos

$$[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!]_{n+1} \equiv [\![\mathrm{N}, \mathrm{Y}_1, \ldots, \mathrm{Y}_m]\!]_{n+1} \text{ (comp } \varphi)$$

sse para todas $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m, \mathrm{X}_{n+1}]\!]_n \in [\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!]_{n+1}$ e $[\![\mathrm{N}, \mathrm{Y}_1, \ldots, \mathrm{Y}_m, \mathrm{Y}_{n+1}]\!]_n \in [\![\mathrm{N}, \mathrm{Y}_1, \ldots, \mathrm{Y}_m]\!]_{n+1}$ vale

$$[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m, \mathrm{X}_{n+1}]\!]_n \equiv [\![\mathrm{N}, \mathrm{Y}_1, \ldots, \mathrm{Y}_m, \mathrm{Y}_{n+1}]\!]_n \text{ (comp } \alpha).$$

Da hipótese de indução, isto é equivalente a $\mathrm{M} \oplus_{\mathrm{L}} \mathrm{N} \models \frac{c_1,\ldots,c_m,c_{n+1}}{x_1,\ldots,x_m,x_{m+n+1}}\alpha$, onde c_{n+1} é o nome do conjunto arbitrário $\mathrm{X}_{n+1} \cup \mathrm{Y}_{n+1}$ em $\mathrm{L_I(M \oplus N)}$. Da Proposição III.2.1, isto é equivalente a $\mathrm{M} \oplus_{\mathrm{L}} \mathrm{N} \models \frac{c_1,\ldots,c_m}{x_1,\ldots,x_m}\varphi$.

O resultado segue do Princípio de Indução. ⊣

Vamos agora discutir uma noção de finitude de índice baseado no que é feito por D. Kozen [8] para linguagens formais reconhecidas por autômatos finitos. Dizemos que uma relação de equivalência R em um conjunto tem *índice finito* quando R particiona o conjunto em um número finito de classes de equivalência desta relação. Se R e S são relações de equivalência em um conjunto, então dizemos que R *refina* S quando $\mathrm{R} \subseteq \mathrm{S}$ [8].

LEMA III.3.7. Suponhamos que R e S sejam relações de equivalência em um conjunto X. Se R refina S e R tem índice finito, então S tem índice finito.

Demonstração. Suponhamos que R tenha índice $|X/R|$ finito e que R refine S. Consideremos os conjuntos quocientes X/R e X/S. Dado $a \in X/R$ existe um único $b \in X/S$ tal que $a \subseteq b$. De fato, isto segue de X/S ser uma partição de X. Suponhamos que $|X/R| < |X/S|$. Neste caso, vemos que $X = \bigcup X/R \subsetneq \bigcup X/S = X$, o que é uma contradição. Segue então que $|X/S| \leq |X/R|$. ⊣

Denotemos por $\langle\rangle$ a lista vazia. A construção recursiva de árvores associadas às matroides empilhadas permite obter a m-árvore $[\![M]\!]_m = [\![M, \langle\rangle]\!]_m$ para cada matroide $M \in \mathrm{Mod}(T_I)$. Dados $m \in \mathbb{N}$ positivo e $M, N \in \mathrm{Mod}(T_I)$, definamos a relação de equivalência $M \simeq_m N$ sse $[\![M]\!]_m = [\![N]\!]_m$. A relação é de fato de equivalência, já que herda as propriedades de reflexividade, simetria, e transitividade da igualdade de m-árvores. A classe $\mathrm{Mod}(T_I)$ é infinita. Podemos restringir a relação $\simeq_m$ a um conjunto infinito X de matroides não-isomorfas duas a duas. O número de m-árvores é no máximo $\sigma_m(m)$, como mostra a Proposição III.3.5. Disto, segue que a restrição de $\simeq_m$ ao conjunto X tem índice finito.

TEOREMA III.3.8 (Índice Finito). [12, Lema 3.1] Para cada $m \in \mathbb{N}$ positivo, a relação $\simeq_m$ refina a relação $\equiv_m$. Em particular, o índice de $\equiv_m$ restrita a um conjunto infinito de matroides não-isomorfas duas a duas é no máximo $\sigma_m(m)$.

Demonstração. Suponhamos que $M \simeq_m N$. Dado $(U, \varphi) \in \mathrm{Mod}(T_I) \times \mathrm{Snt}(L_I)$ tal que φ tem m variáveis e U seja compatível com (M, N), segue do Lema III.3.6 que $U \oplus M \models \varphi$ sse $[\![U]\!]_m \equiv [\![M]\!]_m$ (comp φ). De $[\![M]\!]_m = [\![N]\!]_m$, vemos que $[\![U]\!]_m \equiv [\![M]\!]_m$ (comp φ) sse $[\![U]\!]_m \equiv [\![N]\!]_m$ (comp φ). Novamente do Lema III.3.6, temos $[\![U]\!]_m \equiv [\![N]\!]_m$ (comp φ) sse $U \oplus N \models \varphi$. Disto, obtemos $(U \oplus M)[\varphi] = (U \oplus N)[\varphi]$, e portanto, $M \equiv_m N$. Do Lema III.3.7, vemos que o índice de $\equiv_m$ restrita a um conjunto infinito de matroides não-isomorfas duas a duas é no máximo $\sigma_m(m)$. ⊣

O Teorema III.3.8 é importante, pois ele fornece uma técnica para demonstrar indefinibilidades de propriedades pertinentes às matroides de maneira bem natural. Ele conecta duas atividades, uma de Lógica Monádica de Segunda Ordem e uma de Teoria de Matroides, que precisam ser realizadas para mostrar as indefinibilidades. Vamos explicitar tal técnica e tal conexão na forma do seguinte corolário:

COROLÁRIO III.3.9 (Técnica). Suponhamos que P seja uma propriedade pertinente às matroides e que $\mathcal{M} = \{ M_i : i \in \mathbb{N} \}$ seja um conjunto infinito e enumerável de matroides não-isomorfas duas a duas tal que $M_i \oplus M_j$ tem a propriedade P sse $i = j$[1]. Não existe $\varphi \in \mathrm{Snt}(L_I)$ tal que $M \in \mathrm{Mod}(T_I + \varphi)$ sse $M \in \mathrm{Mod}(T_I)$ tem a propriedade P.

Demonstração. Suponhamos que exista $\varphi \in \mathrm{Snt}(L_I)$ tal que $M \in \mathrm{Mod}(T_I + \varphi)$ sse $M \in \mathrm{Mod}(T_I)$ tem a propriedade P. Por hipótese, o conjunto $\mathcal{M}$ é infinito e enumerável. Do Teorema III.3.8, sabemos que a relação $\equiv_m$ restrita ao conjunto $\mathcal{M}$ tem índice no máximo $\sigma_m(m)$. Disto, segue que existem números naturais $i, j \in \mathbb{N}$ com $i \neq j$ tais que $M_i \equiv_m M_j$. Tomemos $N \cong M_i$ com $E(N) \cap (E(M_i) \cup E(M_j)) = \emptyset$. Por hipótese, sabemos que $N \oplus M_i$ tem a propriedade P e que $N \oplus M_j$ não tem a

[1]Estamos abusando de notação aqui. Quando $i = j$, tomamos cópias isomorfas e disjuntas de uma mesma matroide, já que a definição de soma direta exige que os conjuntos subjacentes sejam disjuntos.

propriedade P. O par (N, φ) não é um m-certificado, e assim, $1 = (N \oplus M_i)[\varphi] = (N \oplus M_j)[\varphi] = 0$, o que é uma contradição. Descartamos a suposição e concluímos sua negação. ⊣

Isto mostra que os esforços agora devem ser direcionados para a construção de conjuntos de matroides linearmente e algebricamente representáveis que atendam às hipóteses do Corolário III.3.9 para que provemos finalmente os resultados que são os objetivos desta dissertação. Isto evidencia a conexão que citamos anteriormente: uma vez estabelecido o resultado lógico do Corolário III.3.9, precisamos agora construir os resultados da Teoria de Matroides que dizem respeito às coleções de interesse. O que segue agora é a obtenção sistemática de tais coleções especiais de matroides. Para o caso da representabilidade linear, vamos explorar a conexão entre matroides e diagramas de pontos e retas. Uma matroide simples M sobre um conjunto E e de posto três pode ser representada geometricamente por pontos e retas em um plano. Primeiro, associamos biunivocamente os elementos de E a pontos no plano. Depois, para cada flat F de M com $3 \leq |F|$ e $r(F) = 2$, traçamos uma reta ligando os pontos do plano que correspondem aos elementos de F. O seguinte lema apresenta condições suficientes para que um tal diagrama represente geometricamente uma matroide simples de posto três.

LEMA III.3.10. [15, Exercício 3 sec. 1.5] Suponhamos que D seja um diagrama envolvendo pontos e retas[m] em um plano que satifaz:

(1) Os conjuntos de pontos e retas de D são disjuntos.

(2) Toda reta contém ao menos dois pontos.

(3) Existem ao menos três pontos não colineares.

(4) Todo par de retas distintas em D se intersecta no máximo em um ponto em comum.

Existe uma matroide simples de posto três sobre o conjunto de pontos de D cujas bases são os cojuntos de três pontos não colineares de D.

Demonstração. Suponhamos que E seja o conjunto dos pontos de D. Vamos definir a coleção $\mathcal{I}$ da seguinte maneira: $X \subseteq E$ é tal que $X \in \mathcal{I}$ sse vale algum dos itens abaixo:

(1) O conjunto X tem no máximo dois pontos de D.

(2) O conjunto X tem três pontos não colineares de D.

A coleção $\mathcal{I}$ é não-vazia e hereditária. Basta mostrar que $\mathcal{I}$ possui a propriedade de aumento. Suponhamos que existam $X, Y \in \mathcal{I}$ com $|X| < |Y|$ tais que para todo $a \in Y - X$ valha $X \cup a \notin \mathcal{I}$. Neste caso, vemos que $|Y| = 3$ e $|X| = 2$. Escrevamos $Y = \{a_1, a_2, a_3\}$ e $X = \{b_1, b_2\}$. Dado $i \in \{1, 2, 3\}$, cada um dos conjuntos $P_i = \{b_1, b_2, a_i\}$ é formado por três pontos colineares, e assim, existe uma reta r_i que incide aos pontos de P_i. As retas r_1, r_2 e r_3 incidem aos pontos b_1 e b_2, e portanto, estas retas têm esses dois pontos em comum. Disto, segue que $r_1 = r_2 = r_3$. Isto implica que a_1, a_2 e a_3 são colineares, o que contradiz $Y \in \mathcal{I}$. O par $(E, \mathcal{I})$ é uma matroide simples. ⊣

[m] A noção de reta usada aqui é abstrata e não coincide necessariamente com a noção Euclidiana de reta (vide a Figura III.3.3).

Vamos agora apresentar uma classe de matroides que são linearmente representáveis sob condições específicas. Utilizando estas matroides e o resultado sobre o índice da relação de m-equivalência, podemos demonstrar que a linguagem $\mathrm{L_I}$ não é capaz de expressar representabilidade linear de matroides.

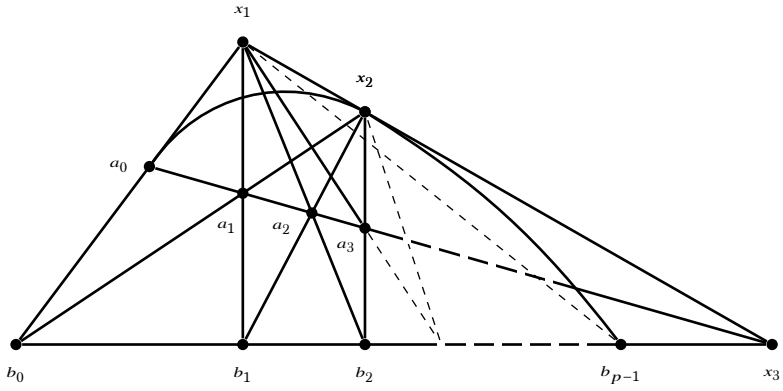

Figura III.3.2: Diagrama que dá origem à matroide M_p do Lema III.3.11.

LEMA III.3.11. [15, Exercício 3(iii) sec. 6.8] Suponhamos que p seja um número primo maior que dois e que M_p seja a matroide cujo diagrama é apresentado na Figura III.3.2. A matroide M_p é linearmente F-representável sse F tem característica p.

Demonstração. O posto de M_p é três. Suponhamos que F seja um corpo de característica prima q e que a matriz

$$\mathrm{A}_p = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & a_0 & b_0 & a_1 & b_1 & a_2 & b_2 & \cdots & a_{p-1} & b_{p-1} \end{matrix} \\ \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 & r_{1,1} & r_{1,2} & \cdots & r_{1,p-1} & r_{2,p-1} \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & s_{1,1} & s_{1,2} & \cdots & s_{1,p-1} & s_{2,p-1} \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & t_{1,1} & t_{1,2} & \cdots & t_{1,p-1} & r_{2,p-1} \end{bmatrix} \end{array}$$

represente a matroide M_p sobre F. A matriz A_p tem $2p + 3$ colunas. Do diagrama, sabemos que o conjunto $\{ a_0, x_2, b_1 \}$ é independente, e portanto, os vetores $(1, 1, 0)$, $(1, 0, 1)$ e $(0, 1, 1)$ são linearmente independentes. Temos

$$\det \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = -2,$$

e assim, $2 < q$. Do diagrama, obtemos o seguinte:

(1) O conjunto $\{ a_0, x_3, a_i \}$ é dependente para cada $i \in \{ 1, \ldots, p-1 \}$, e portanto, o determinante da submatriz

$$\begin{bmatrix} 1 & 0 & r_{1,i} \\ 1 & 0 & s_{1,i} \\ 0 & 1 & t_{1,i} \end{bmatrix}$$

é nulo. Usando a primeira para a expansão do determinante, obtemos $s_{1,i} = 1$ para todo $i \in \{ 1, \ldots, p-1 \}$. Usando a última linha para a expansão do mesmo determinante, obtemos $r_{1,i} = s_{1,i}$ para todo $i \in \{ 1, \ldots, p-1 \}$. O conjunto $\{ b_0, x_3, b_i \}$ é

dependente para cada $i \in \{1, \ldots, p-1\}$, e portanto, o determinante da submatriz

$$\begin{bmatrix} 0 & 0 & r_{2,i} \\ 1 & 0 & s_{2,i} \\ 0 & 1 & t_{2,i} \end{bmatrix}$$

é nulo. Usando a primeira para a expansão do determinante, obtemos $r_{2,i} = 0$ para todo $i \in \{1, \ldots, p-1\}$. O conjunto $\{x_1, x_2, b_i\}$ é independente para todo $i \in \{1, \ldots, p-1\}$. Disto, obtemos

$$\det \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & s_{2,i} \\ 0 & 1 & t_{2,i} \end{bmatrix} = -s_{2,i},$$

e portanto, $s_{2,i} \neq 0$ para cada $i \in \{1, \ldots, p-1\}$. Multiplicando as colunas com rótulos $b_1, \ldots, b_{p-1}$ por escalares, se necessário, podemos supor que $s_{2,i} = 1$ para cada $i \in \{1, \ldots, p-1\}$.

(2) O conjunto $\{x_1, a_i, b_i\}$ é dependente para cada $i \in \{1, \ldots, p-1\}$. Disto, obtemos

$$0 = \det \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & t_{1,i} & t_{2,i} \end{bmatrix} = t_{2,i} - t_{1,i},$$

e portanto, $t_{1,i} = t_{2,i} = t_i$ para cada $i \in \{1, \ldots, p-1\}$. O conjunto $\{x_2, b_1, a_2\}$ é dependente, e assim,

$$0 = \det \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & t_2 \end{bmatrix} = t_i - 2.$$

Isto mostra que $t_2 = 2$. Suponhamos que para cada $i < p-1$, valha $t_i = i$. O conjunto $\{x_2, b_i, a_{i+1}\}$ é dependente, e assim,

$$0 = \det \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & i & t_{i+1} \end{bmatrix} = t_{i+1} - i - 1.$$

Isto mostra que $t_{i+1} = i + 1$.

A matriz A_p tem a seguinte forma:

$$\mathrm{A}_p = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & a_0 & b_0 & a_1 & b_1 & a_2 & b_2 & \cdots & a_{p-1} & b_{p-1} \end{matrix} \\ \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 2 & 2 & \cdots & p-1 & p-1 \end{bmatrix} \end{array}$$

Se valesse $q < p$, então alguma coluna seria repetida, o que contradiria a simplicidade de M_p. Isto mostra que $p \leq q$. Por fim, vemos que o conjunto $\{a_0, x_2, b_{p-1}\}$ é dependente sse $q = p$, uma vez que vale:

$$\det \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & p-1 \end{bmatrix} = -p. \qquad \dashv$$

Para cada número primo p maior que dois, tomemos a matroide M_p^- obtida de M_p exigindo que o conjunto $\{ a_0, x_2, b_{p-1} \}$ seja uma base. A matroide M_p^- é linearmente F-representável sse a característica de F é zero ou maior que p. Usando o resultado do lema anterior e do Teorema III.3.8, obtemos o seguinte resultado que demonstra que a linguagem L_I não é capaz de definir as classes de matroides linearmente representáveis. Já sabemos como definir as matroides M_p e M_p^- para cada número primo p maior que dois. O seguinte lema permite estender estas classes com mais duas matroides que dão conta do caso em que supomos que o corpo tem característica dois.

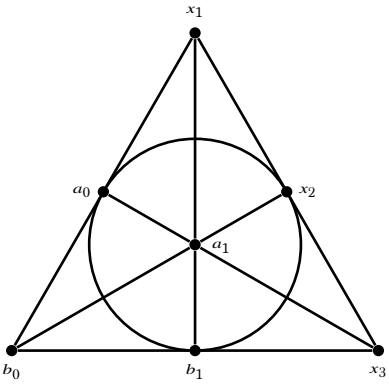

Figura III.3.3: A figura apresenta o diagrama da matroide M_2. A matroide M_2 é denotada por F_7 em alguns textos de matroide (vide J. Oxley [15]) e é chamada de *matroide de Fano.*

LEMA III.3.12. Suponhamos que M_2 seja a matroide cujo diagrama é apresentado na Figura III.3.3. A matroide M_2 é linearmente F-representável sse F tem característica dois.

Demonstração. O posto de M_2 é três. Suponhamos que F seja um corpo de característica q e que a matriz

$$A_2 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & a_0 & b_0 & a_1 & b_1 \end{matrix} \\ \begin{bmatrix} 1 & r_1 & 0 & s_1 & 0 & 1 & t_1 \\ 0 & r_2 & 0 & s_2 & 1 & 1 & t_2 \\ 0 & r_3 & 1 & s_3 & 0 & 1 & t_3 \end{bmatrix} \end{array}$$

represente a matroide M_2 sobre F. A matriz A_2 tem 7 colunas. Procedendo com uma análise semelhante àquela feita na demonstração do Lema III.3.11, obtemos:

$$A_2 = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & a_0 & b_0 & a_1 & b_1 \end{matrix} \\ \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

Por fim, o conjunto $\{ a_0, x_2, b_1 \}$ é dependente sse $q = 2$, uma vez que vale:

$$\det \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = -2. \qquad \dashv$$

Tomemos a matroide M_2^- obtida de M_2 exigindo que o conjunto $\{a_0, x_2, b_1\}$ seja uma base. A matroide M_2^- é linearmente F-representável sse a característica de F é diferente de dois. Dos resultados dos Lemas III.3.11 e III.3.12, obtemos conjuntos infinitos e enumeráveis de matroides que atendem às hipóteses do Corolário III.3.9. Os seguintes resultados seguem imediatamente da técnica apesentada no referido corolário.

COROLÁRIO III.3.13.

(1) [12, Teorema 1.1] Não existe $\varphi \in \mathrm{Snt}(L_I)$ tal que $M \in \mathrm{Mod}(T_I + \varphi)$ sse $M \in \mathrm{Mod}(T_I)$ é linearmente representável.

(2) Dado um número primo p, não existe $\varphi \in \mathrm{Snt}(L_I)$ tal que $M \in \mathrm{Mod}(T_I + \varphi)$ sse $M \in \mathrm{Mod}(T_I)$ é linearmente representável sobre um corpo de característica maior que p.

(3) Dado um número natural n, não existe $\varphi_n \in \mathrm{Snt}(L_I)$ tal que $M \in \mathrm{Mod}(T_I + \varphi_n)$ sse $M \in \mathrm{Mod}(T_I)$ é linearmente representável sobre um corpo com mais de n elementos.

III.4 INDEFINIBILIDADE: SEGUNDA PARTE

Vamos apresentar nesta seção a indefinibilidade da representabilidade algébrica na linguagem L_I. Esta é uma contribuição desta dissertação e ela estende os resultados provados por D. Mayhew, M. Newman e G. Whittle [12]. As referências principais desta seção são D. J. Winter [22], J. Oxley [15] e B. Lindström [11]. Como um público potencial desta dissertação é formado por pessoas estudantes de Ciência da Computação, vamos apresentar as noções básicas de extensões de corpos utilizadas na obtenção de matroides neste contexto algébrico.

Um *extensão* de um corpo k é um corpo F que contém k como subcorpo juntamente com uma estrutura de espaço vetorial sobre k. Escrevemos $k \subseteq F$ para denotar que F é uma extensão de k. O *grau* de uma extensão $k \subseteq F$ é a dimensão $(F : k) = \dim_k F$ de F sobre k. Vamos escrever $(F : k) < \aleph_0$ para indicar que a extensão tem grau finito. Uma *subextensão* de uma extensão $k \subseteq F$ de um corpo k é um corpo k' que estende k e é estendido por F, i.e. tal que existem as extensões $k \subseteq k'$ e $k' \subseteq F$. O seguinte resultado de demonstração rotineira mostra que os graus de extensões podem ser fatorados quando existem subextensões.

PROPOSIÇÃO III.4.1. [22, Proposição 1.1.7] Se V é um espaço vetorial sobre F e $k \subseteq F$ é um extensão de corpos, então $(V : k) = (V : F)(F : k)$.

Se $k \subseteq F$ é uma extensão e $S \subseteq F$ é um subconjunto de elementos de F, então denotamos por $k\langle S\rangle$, $k[S]$ e $k(S)$ as interseções de todos os subespaços vetoriais de F sobre k que contém S, de todos os subaneis de F que contém k e S e de todos os subcorpos de F que contém k e S, respectivamente. Quando existe um número natural positivo m tal que $S = \{s_1, \ldots, s_m\}$, então escrevemos $k\langle s_1, \ldots, s_m\rangle$, $k[s_1, \ldots, s_m]$ e $k(s_1, \ldots, s_m)$ no lugar de $k\langle S\rangle$, $k[S]$ e $k(S)$, respectivamente.

LEMA III.4.2. [22, Proposição 1.1.9] Se $k \subseteq F$ é uma extensão de corpos e $S \subseteq F$, então tomemos S_{fin} a coleção dos subconjuntos finitos de S. Vale $k(S) = \bigcup_{T \in S_{\mathrm{fin}}} k(T)$. Analogamente para $k\langle S\rangle$ e $k[S]$.

Demonstração. Dado $T \in S_{fin}$, sabemos que $k(T)$ é a interseção de todos os subcorpos de F que contém k e T. Em particular, $k(S)$ é um subcorpo de F que contém k e T, e assim, $k(T) \subseteq k(S)$. Isto mostra que $\bigcup_{T \in S_{fin}} k(T) \subseteq k(S)$. Por outro lado, se $T \in S_{fin}$, então $k \subseteq k(T)$. Isto mostra que $k \subseteq \bigcup_{T \in S_{fin}} k(T)$. Agora, para cada $s \in S$, sabemos que $k(s)$ é a interseção de todos os subcorpos de F que contém k e s. Assim, $S \subseteq \bigcup_{T \in S_{fin}} k(T)$. Dados $a, b \in \bigcup_{T \in S_{fin}} k(T)$, existem $A, B \in S_{fin}$ tais que $a \in k(A)$ e $b \in k(B)$, e portanto, $a + b, a - b, a \cdot b \in k(A \cup B) \subseteq \bigcup_{T \in S_{fin}} k(T)$ e $a^{-1} \in k(A) \subseteq \bigcup_{T \in S_{fin}} k(T)$ quando $a \neq 0$. Disto, vemos que $\bigcup_{T \in S_{fin}} k(T)$ é um subcorpo de F que contém k e S. Isto mostra que $k(S) \subseteq \bigcup_{T \in S_{fin}} k(S)$. ⊣

Suponhamos que $k \subseteq F$ seja uma extensão de um corpo k. Quando $F = k(s)$, dizemos que $k \subseteq k(s)$ é uma ***extensão simples*** e que o elemento $s \in F$ é um ***elemento primitivo*** da extensão. Suponhamos que $k[X]$ seja o anel de polinômios com coeficientes em k e indeterminada X. Existe o homomorfismo avaliação $ev_s : k[X] \longrightarrow k[s]$ que mapeia um polinômio $p(X) = a_m X^m + \cdots + a_1 X + a$ de $k[X]$ no elemento $p(s) = a_m s^m + \cdots + a_1 s + a_0$ de $k[s]$. O subanel $k[s]$ de $k(s)$ é um domínio de integridade, e portanto, $I = \ker(ev_s)$ é um ideal primo de $k[X]$. Se ev_s é injetiva, então dizemos que s é ***transcendente*** sobre k. Se ev_s não é injetiva, então existe $p(X) \in k[X]$ não-identicamente nulo tal que $p(s) = 0$. Neste caso, dizemos que s é ***algébrico*** sobre k. No caso em que s é algébrico, segue de $k[X]$ ser um domínio principal que existe $\mu_s(X) \in K[X]$ irredutível de menor grau e com coeficiente líder igual a um tal que $I = \mu_s(X)k[X]$. O polinômio $\mu_s(X)$ é denominado ***polinômio mínimo*** de a em $k[X]$. O seguinte resultado resume o que foi discutido:

PROPOSIÇÃO III.4.3. [22, Proposição 1.1.13] Suponhamos que $k \subseteq F$ seja uma extensão de um corpo k e que $s \in F$.

(1) Se s é transcendente sobre k, então $k(s)$ é k-isomorfo ao corpo de frações do domínio $k[X]$.

(2) Se s é algébrica sobre k, então $k(s) = k[s] = k\langle 1, s, \ldots, s^{m-1} \rangle$ é k-isomorfo ao corpo quociente $k[X]/\mu_s(X)k[X]$ de modo que $(k(s) : k) = m$, onde m é o grau de seu polinômio mínimo $\mu_s(X)$.

Segue da Proposição III.4.1 que uma extensão simples $k \subseteq k(s)$ é algébrica sse $(k(s) : k) < \aleph_0$. Uma extensão de corpos $k \subseteq F$ é ***algébrica*** quando as extensões simples $k \subseteq k(s)$ são algébricas para cada $s \in F$.

LEMA III.4.4. Suponhamos que $k \subseteq F$ seja uma extensão de um corpo k.

(1) [22, Proposição 1.2.2] Um elemento $s \in F$ é algebrico sobre k sse existem extensões $k \subseteq k' \subseteq F$ tais que $(k', k) < \aleph_0$ e $s \in k'$.

(2) [22, Proposição 1.2.3] Suponhamos que $S \subseteq F$ seja um subconjunto finito de elementos de F. Todo elemento de S é algébrico sobre k sse $(k(S) : k) < \aleph_0$.

Demonstração.

(1) Se s é algébrico, basta tomar $k' = k(s)$. Suponhamos que $k \subseteq k'$ seja tal que $(k', k) < \aleph_0$ e $s \in k'$. Temos as extensões $k \subseteq k(s) \subseteq k'$. Da Proposição III.4.1, temos $(k' : k) = (k' : k(s))(k(s) : k)$. Como $(k', k) < \aleph_0$, vemos que $(k(s), k) < \aleph_0$. Como $k \subseteq k(s)$ é simples e finita, vemos que s é algébrico sobre k.

(2) Suponhamos que $(k(\mathrm{S}) : k) < \aleph_0$. Temos as extensões $k \subseteq k(s) \subseteq k(\mathrm{S})$ para cada $s \in \mathrm{S}$. Da Proposição III.4.1, temos $(k(\mathrm{S}) : k) = (k(\mathrm{S}) : k(s))(k(s) : k)$. Como $(k(\mathrm{S}), k) < \aleph_0$, vemos que $(k(s), k) < \aleph_0$. Do primeiro item, segue que s é algébrico sobre k. Isto mostra a volta. Provemos a ida por indução no número de elementos de S. Se $|\mathrm{S}| = 1$, então o resultado vale pelo primeiro item. Suponhamos que o resultado seja válido para todo subconjunto de F com menos de $|\mathrm{S}|$ elementos algébricos sobre k. Dado $s \in \mathrm{S}$, tomemos as extensões $k \subseteq k(s) \subseteq k(s)(\mathrm{S}-s)$. Da hipótese de indução sabemos que todo elemento de $\mathrm{S}-s$ é algébrico sobre k sse $(k(\mathrm{S}-s) : k) < \aleph_0$. Por hipótese, todo elemento de S é algébrico sobre k, e portanto, $(k(s) : k) < \aleph_0$ e $(k(\mathrm{S}-s) : k) < \aleph_0$. Da Proposição III.4.1, obtemos $(k(s)(\mathrm{S} - s) : k) < \aleph_0$. De $k(s)(\mathrm{S} - s) = k(\mathrm{S})$ e do Princípio de Indução, obtemos o resultado. ⊣

PROPOSIÇÃO III.4.5. [22, Proposição 1.2.7] Uma extensão $k \subseteq \mathrm{F}$ é algébrica sse qualquer uma de suas subextensões é algébrica.

Demonstração. Suponhamos que $k \subseteq k' \subseteq \mathrm{F}$ sejam extensões de corpos. Primeiro, provemos a volta. Se $k \subseteq \mathrm{F}$ é algébrica, então todo elemento de F é algébrico sobre k, e portanto, todo elemento de k' é algébrico sobre k. Dado $s \in \mathrm{F}$, sabemos que $k \subseteq k(s)$ é algébrica. Disto, existe o polinômio mínimo $\mu_s(\mathrm{X}) \in k[\mathrm{X}] \subseteq k'[\mathrm{X}]$ tal que $\mu_s(s) = 0$, e assim, $k' \subseteq k'(s)$ é algébrica. Disto, vemos que $k' \subseteq \mathrm{F}$ é algébrica. Provemos agora a ida. Suponhamos que as extensões $k \subseteq k'$ e $k' \subseteq \mathrm{F}$ sejam algébricas. Dado $s \in \mathrm{F}$, devemos mostrar que a extensão $k \subseteq k(s)$ é algébrica. Por hipótese, sabemos que $k' \subseteq \mathrm{F}$ é algébrica. Tomemos $\mu_s(\mathrm{X}) \in k'[\mathrm{X}]$ o polinômio mínimo de s em $k'[\mathrm{X}]$ e denotemos por S o conjunto dos coeficientes de $\mu_s(\mathrm{X})$. Por hipótese, sabemos que $k \subseteq k'$ é algébrica, e assim, todo elemento de S é algébrico sobre k. Do segundo item do Lema III.4.4, vemos que $(k(\mathrm{S}) : k) < \aleph_0$. Isto permite obter as extensões $k \subseteq k(\mathrm{S})(s)$ e $k(\mathrm{S})(s) \subseteq \mathrm{F}$. Em virtude do primeiro item do Lema III.4.4, devemos mostrar que $(k(\mathrm{S})(s), k) < \aleph_0$. A extensão $k(\mathrm{S}) \subseteq k(\mathrm{S})(s)$ é algébrica, pois $\mu_s(\mathrm{X}) \in k(\mathrm{S})[\mathrm{X}]$ é o polinômio mínimo de s em $k(\mathrm{S})[\mathrm{X}]$. Como $k(\mathrm{S}) \subseteq k(\mathrm{S})(s)$ é simples e algébrica, vemos que $(k(\mathrm{S})(s) : k(\mathrm{S})) < \aleph_0$. Obtemos as extensões $k \subseteq k(\mathrm{S}) \subseteq k(\mathrm{S})(s)$. Sabemos que $(k(\mathrm{S}) : k) < \aleph_0$ e $(k(\mathrm{S})(s) : k(\mathrm{S})) < \aleph_0$. Da Proposição III.4.1, obtemos $(k(\mathrm{S})(s), k) < \aleph_0$. Do primeiro item do Lema III.4.4, segue que s é algébrico sobre k. Como $s \in \mathrm{F}$ é arbitrário, vemos que a extensão $k \subseteq \mathrm{F}$ é algébrica. ⊣

Suponhamos que $k \subseteq \mathrm{F}$ seja uma extensão de um corpo k, que $a \in \mathrm{F}$ e que $\mathrm{S}, \mathrm{T} \subseteq \mathrm{F}$. Dizemos que a é *k-algebricamente dependente* sobre S em F e escrevemos $a \preceq \mathrm{S}$ quando a é algébrico sobre $k(\mathrm{S})$. Isto quer dizer que a subextensão simples $k(\mathrm{S}) \subseteq k(\mathrm{S})(a)$ da extensão $k \subseteq \mathrm{F}$ é algébrica, e portanto, existe $p(\mathrm{X}) \in k(\mathrm{S})[\mathrm{X}]$ tal que $p(a) = 0$. Disto, vemos que $(k(\mathrm{S})(a) : k(\mathrm{S})) < \aleph_0$. Dizemos que S é *$k$-algebricamente dependente* sobre T em F e escrevemos $\mathrm{S} \preceq \mathrm{T}$ quando vale $s \preceq \mathrm{T}$ para todo $s \in \mathrm{S}$.

PROPOSIÇÃO III.4.6. [22, Teorema 1.6.2] Suponhamos que $k \subseteq \mathrm{F}$ seja uma extensão de um corpo k, que $a, b \in \mathrm{F}$ e que $\mathrm{S}, \mathrm{T} \subseteq \mathrm{F}$.

(1) Para todo $s \in \mathrm{S}$, vale $s \preceq \mathrm{S}$.

(2) Se $a \preceq \mathrm{S}$, então existe um subconjunto finito $\mathrm{S}_0 \subseteq \mathrm{S}$ tal que $a \preceq \mathrm{S}_0$.

(3) Se $a \preceq \mathrm{S}$ e $\mathrm{S} \preceq \mathrm{T}$, então $a \preceq \mathrm{T}$.

(4) Se $a \preceq \mathrm{S}$ e $a \not\preceq \mathrm{S} - b$, então $b \preceq (\mathrm{S} - b) \cup a$.

Demonstração.

(1) Dado $s \in \mathrm{S}$, temos $s \in k(\mathrm{S})$. Temos $\mu_s(\mathrm{X}) = \mathrm{X} - s$ o polinômio mínimo de s em $k(\mathrm{S})[\mathrm{X}]$, e portanto, a extensão simples $k(\mathrm{S}) \subseteq k(\mathrm{S})(s) = k(\mathrm{S})$ é algébrica. Disto, vemos que $s \preceq \mathrm{S}$.

(2) Suponhamos que $a \preceq \mathrm{S}$. Disto, vemos que a é algébrico sobre $k(\mathrm{S})$. Existe $\mu_a(\mathrm{X}) \in k(\mathrm{S})[\mathrm{X}]$ o polinômio mínimo de a em $k(\mathrm{S})[\mathrm{X}]$. Tomemos A o conjunto cujos elementos são os coeficientes de $\mu_a(\mathrm{X})$. Do Lema III.4.2, sabemos que $k(\mathrm{S}) = \bigcup_{\mathrm{T} \in \mathrm{S}_{\mathrm{fin}}} k(\mathrm{T})$. Como A é finito, existe $\mathrm{S}_0 \subseteq \mathrm{S}$ finito tal que $\mathrm{A} \subseteq k(\mathrm{S}_0)$. Disto, podemos construir $\mu_a(\mathrm{X})$ em $k(\mathrm{S}_0)[\mathrm{X}]$. Como $\mu_a(a) = 0$, vemos que a é algébrico sobre $k(\mathrm{S}_0)$. Isto mostra que $a \preceq \mathrm{S}_0$.

(3) Suponhamos que valham $a \preceq \mathrm{S}$ e $\mathrm{S} \preceq \mathrm{T}$. Do item anterior, sabemos que existe $\mathrm{S}_0 \subseteq \mathrm{S}$ finito tal que $a \preceq \mathrm{S}_0$. De $\mathrm{S} \preceq \mathrm{T}$, obtemos $\mathrm{S}_0 \preceq \mathrm{T}$, e assim, $(k(\mathrm{T}) : k(\mathrm{T})(s)) < \aleph_0$ para todo $s \in \mathrm{S}_0$. Isto mostra que todo elemento de S_0 é algébrico sobre $k(\mathrm{T})$. Do Lema III.4.4, vemos que $(k(\mathrm{T})(\mathrm{S}_0) : k(\mathrm{T})) < \aleph_0$. De $a \preceq \mathrm{S}_0$, temos $(k(\mathrm{S}_0)(a) : k(\mathrm{S}_0)) < \aleph_0$. Existe $\mu_a(\mathrm{X}) \in k(\mathrm{S}_0)[\mathrm{X}]$ o polinômio mínimo de a em $k(\mathrm{S}_0)[\mathrm{X}]$. Como $k(\mathrm{S}_0)[\mathrm{X}] \subseteq k(\mathrm{T})(\mathrm{S}_0)[\mathrm{X}]$, temos $(k(\mathrm{T})(\mathrm{S}_0)(a) : k(\mathrm{T})(\mathrm{S}_0)) < \aleph_0$. Obtemos, por fim, as extensões:

$$k(\mathrm{T}) \subseteq k(\mathrm{T})(\mathrm{S}_0) \subseteq k(\mathrm{T})(\mathrm{S}_0)(a)$$
$$k(\mathrm{T}) \subseteq k(\mathrm{T})(a) \subseteq k(\mathrm{T})(\mathrm{S}_0)(a).$$

Por um lado, segue da Proposição III.4.1 que

$$(k(\mathrm{T})(\mathrm{S}_0)(a) : k(\mathrm{T})) = (k(\mathrm{T})(\mathrm{S}_0)(a) : k(\mathrm{T})(a))(k(\mathrm{T})(a) : k(\mathrm{T})).$$

Por outro lado, segue da Proposição III.4.1 que

$$(k(\mathrm{T})(\mathrm{S}_0)(a) : k(\mathrm{T})) = (k(\mathrm{T})(\mathrm{S}_0)(a) : k(\mathrm{T})(\mathrm{S}_0))(k(\mathrm{T})(\mathrm{S}_0) : k(\mathrm{T})).$$

Provamos que $(k(\mathrm{T})(\mathrm{S}_0) : k(\mathrm{T})) < \aleph_0$ e $(k(\mathrm{T})(\mathrm{S}_0)(a) : k(\mathrm{T})(\mathrm{S}_0)) < \aleph_0$, e assim, $(k(\mathrm{T})(\mathrm{S}_0)(a) : k(\mathrm{T})) < \aleph_0$. Isto mostra que $(k(\mathrm{T})(a) : k(\mathrm{T})) < \aleph_0$. Concluímos que a é algébrico sobre $k(\mathrm{T})$, e portanto, $a \preceq \mathrm{T}$.

(4) Suponhamos que $a \preceq \mathrm{S}$ e que $a \not\preceq \mathrm{S} - b$. Neste caso, vemos que a é algébrico sobre $k(\mathrm{S})$ e não é algébrico sobre $k(\mathrm{S} - b)$. Devemos mostrar que b é algébrico sobre $k(\mathrm{S}-b)(a)$. Existe $p(\mathrm{X}) = a_m(b)\mathrm{X}^m + \cdots a_1(b)\mathrm{X} + a_0(b)$ não identicamente nulo em $k(\mathrm{S} - b)(b)[\mathrm{X}] = k(\mathrm{S})[\mathrm{X}]$ tal que $p(a) = 0$. Partindo de $a_m(b)a^m + \cdots a_1(b)a + a_0(b) = 0$, podemos obter $b_m(b)a^m + \cdots + b_1(b)a + b_0 = 0$ multiplicando por um fator que torne todos os denominadores dos coeficientes iguais a um. Para cada $i \in \{0, 1, \ldots, m\}$, podemos escrever $b_i(b) = c_{i,m_i} b^{m_i} + \cdots + c_{i,1} b + c_{i,0}$ com $c_{i,0}, \ldots, c_{i,m_i} \in k(\mathrm{S} - b)$ e $c_{i,m_i} \neq 0$. Disto obtemos:

$$0 = \sum_{i=0}^{m} b_i(b) a^i = \sum_{i=0}^{m} \sum_{r=1}^{m_i} c_{i,r} b^r a^i = \sum_{j=0}^{n} \sum_{s=1}^{n_i} c_{j,s} a^s b^j = \sum_{j=0}^{n} b_j(a) b^j$$

para algum número natural n. Existe $j \in \{0, 1, \ldots, n\}$ tal que $b_j(a) \neq 0$. De fato, suponhamos que para todo $j \in \{0, 1, \ldots, n\}$ valha $b_j(a) = 0$. Existe $b_j(\mathrm{X}) \in$

$k(\mathrm{S}-b)[\mathrm{X}]$ que se anula em a. De $a \not\preceq \mathrm{S}-b$, segue que $b_j(\mathrm{X})$ é identicamente nulo para todo $j \in \{0,1,\ldots,m\}$. Disto, segue que $p(\mathrm{X})$ é identicamente nulo, o que é uma contradição. Obtemos assim um polinômio não identicamente nulo $q(\mathrm{X}) = b_n(a)\mathrm{X}^n + \cdots + b_1(a)\mathrm{X} + b_0(a)$ em $k((\mathrm{S}-b)\cup a)[\mathrm{X}]$ tal que $q(b) = 0$. Isto mostra que $b \preceq (\mathrm{S}-b)\cup a$. ⊣

Suponhamos que $k \subseteq \mathrm{F}$ seja uma extensão de um corpo k e que $\mathrm{S} \subseteq \mathrm{F}$. Dizemos que S é *$k$-algebricamente independente* em F quando $s \not\preceq \mathrm{S}-s$ para todo $s \in \mathrm{S}$. Um extensão $k \subseteq \mathrm{F}$ é *puramente transcendente* quando existe um conjunto k-algebricamente independente $\mathrm{S} \subseteq \mathrm{F}$ tal que $\mathrm{F} = k(\mathrm{S})$. Neste caso, dizemos que $k(\mathrm{S})$ é um corpo de *expressões racionais* sobre os elementos de S.

LEMA III.4.7. Suponhamos que $k \subseteq \mathrm{F}$ seja uma extensão de um corpo k. Valem os seguintes resultados:

(1) [22, Proposição 1.6.8] Suponhamos que $\mathrm{S} \subseteq \mathrm{T} \subseteq \mathrm{F}$ sejam subconjuntos do corpo F. Se T é k-algebricamente independente em F e $\mathrm{T} \preceq \mathrm{S}$, então $\mathrm{S} = \mathrm{T}$.

(2) [22, Proposição 1.6.9] Suponhamos que $a \in \mathrm{F}$ e que $\mathrm{S} \subseteq \mathrm{F}$. Se o conjunto S é k-algebricamente independente em F e $a \not\preceq \mathrm{S}$, então $\mathrm{S}\cup a$ é k-algebricamente independente em F.

(3) [22, Proposição 1.6.10] Suponhamos que $\mathcal{S} = \{\mathrm{S}_i : i \in \mathrm{I}\}$ seja uma $\subseteq$-cadeia de subconjuntos do corpo F. Se todo elemento de $\mathcal{S}$ é k-algebricamente independente em F, então $\bigcup \mathcal{S}$ é k-algebricamente independente em F.

Demonstração.

(1) Dado $t \in \mathrm{T}$, sabemos que $t \not\preceq \mathrm{T}-t$. Disto, vemos que $t \not\preceq \mathrm{S}-t$. De $\mathrm{T} \preceq \mathrm{S}$, segue que $t \preceq \mathrm{S}$. Se $t \notin \mathrm{S}$, então $\mathrm{S}-t = \mathrm{S}$, e assim, $t \not\preceq \mathrm{S}-t = \mathrm{S}$, o que é uma contradição. Temos $t \in \mathrm{S}$, e portanto, $\mathrm{T} \subseteq \mathrm{S}$. Concluímos que $\mathrm{S} = \mathrm{T}$.

(2) Suponhamos que exista $b \in \mathrm{S}\cup a$ tal que $b \preceq (\mathrm{S}\cup a)-b$. Se $a = b$, então $a \preceq \mathrm{S}$, o que contradiz a hipótese $a \not\preceq \mathrm{S}$. Disto, temos $a \neq b$, e assim, $b \in \mathrm{S}$. Temos $b \preceq \mathrm{S}$ e $b \preceq (\mathrm{S}\cup a)-b = (\mathrm{S}-b)\cup a$. De S ser k-algebricamente independente, temos $b \not\preceq \mathrm{S}-b$. Escrevamos $\mathrm{T} = (\mathrm{S}-b)\cup a$. Temos $b \preceq \mathrm{T}$ e $b \not\preceq \mathrm{T}-a$. Do quarto item da Proposição III.4.6, obtemos $a \preceq (\mathrm{T}-a)\cup b = \mathrm{S}$, o que contradiz a hipótese $a \not\preceq \mathrm{S}$. Desta contradição, concluímos que $\mathrm{S}\cup a$ é k-algebricamente independente em F. ⊣

(3) Tomemos $\mathrm{S} = \bigcup \mathcal{S}$. Suponhamos que exista $s \in \mathrm{S}$ tal que $s \preceq \mathrm{S}-s$. Do segundo item da Proposição III.4.6, existe $\mathrm{S}_0 \subseteq \mathrm{S}-s$ finito tal que $s \preceq \mathrm{S}_0$. Podemos escrever $\mathrm{S}_0 = \{s_1,\ldots,s_m\}$ para algum número natural positivo m. Existem S_1, …, S_m, $\mathrm{S}_{m+1} \in \mathcal{S}$ tais que $a_1 \in \mathrm{S}_1$, …, $a_m \in \mathrm{S}_m$ e $s \in \mathrm{S}_{m+1}$. Como $\{\mathrm{S}_1,\ldots,\mathrm{S}_m,\mathrm{S}_{m+1}\} \subseteq \mathcal{S}$ e $\mathcal{S}$ é uma cadeia, existe $n \in \{1,\ldots,m,m+1\}$ tal que $\mathrm{S}_i \subseteq \mathrm{S}_n$ para cada $i \in \{1,\ldots,m,m+1\}$. Disto, obtemos $s \in \mathrm{S}_n$ e $\mathrm{S}_0 \subseteq \mathrm{S}_n$. De $s \preceq \mathrm{S}_0$ e $\mathrm{S}_0 \subseteq \mathrm{S}_n - s$, segue que $s \preceq \mathrm{S}_n - s$, o que é uma contradição com S_n ser k-algebricamente independente em F. Concluímos que S é k-algebricamente independente em F.

Uma *base de transcendência* de uma extensão $k \subseteq \mathrm{F}$ é um subconjunto $\mathrm{S} \subseteq \mathrm{F}$ que é k-algebricamente independente em F e tal que $k(\mathrm{S}) \subseteq \mathrm{F}$ é uma extensão algébrica.

LEMA III.4.8. [22, Teorema 1.6.11] Suponhamos que $k \subseteq \mathrm{F}$ seja uma extensão de um corpo k. Existe uma base de transcendência de $k \subseteq \mathrm{F}$.

Demonstração. Vamos mostrar que se $\mathrm{T} \subseteq \mathrm{F}$, então existe $\mathrm{S} \subseteq \mathrm{T}$ tal que S é k-algebricamente independente em F e $\mathrm{T} \preceq \mathrm{S}$. Dado $\mathrm{T} \subseteq \mathrm{F}$, tomemos $\mathcal{P}$ o conjunto parcialmente ordenado por $\subseteq$ dos subconjuntos k-algebricamente independentes em F contidos em T. Tomemos $\mathcal{S} \subseteq \mathcal{P}$ uma $\subseteq$-cadeia qualquer. Do terceiro item do Lema III.4.7, sabemos que $\bigcup \mathcal{S}$ é um subconjunto k-algebricamente independente em F contido em T, e portanto, $\bigcup \mathcal{S}$ é uma cota superior de $\mathcal{S}$ em $\mathcal{P}$. Do Lema de Zorn[n], existe um elemento maximal S em $\mathcal{P}$. Vamos mostrar que $\mathrm{T} \preceq \mathrm{S}$. Se $\mathrm{T} \not\preceq \mathrm{S}$, então existe $t \in \mathrm{T}$ que não é algébrico sobre $k(\mathrm{S})$. Do segundo item do Lema III.4.7, obtemos $\mathrm{S} \cup t \in \mathcal{P}$ e $\mathrm{S} \subsetneq \mathrm{S} \cup t$, o que contradiz a maximalidade de S em $\mathcal{P}$. Fazendo T = F, obtemos uma base de transcendência de $k \subseteq \mathrm{F}$. ⊣

O Teorema III.4.9 a seguir mostra que bases de transcendência de extensões de corpos são equicardinais. Ele será útil para definir matroides algébricas partindo de extensões de corpos com bases de transcendência finitas.

TEOREMA III.4.9. [22, Teorema 1.6.12] Suponhamos que $k \subseteq \mathrm{F}$ seja uma extensão de um corpo k. Quaisquer duas bases de transcendência de $k \subseteq \mathrm{F}$ são equicardinais.

Demonstração. Sabemos do Lema III.4.8 que existe uma base de transcendência de $k \subseteq \mathrm{F}$. Suponhamos que S e T sejam duas bases de transcendência de $k \subseteq \mathrm{F}$. Vamos dividir a demonstração em dois casos:

(1) Suponhamos que S e T sejam duas bases infinitas. Da definição de base de transcendência, sabemos que $k(\mathrm{S}) \subseteq \mathrm{F}$ e $k(\mathrm{T}) \subseteq \mathrm{F}$ são algébricas. Dado $t \in \mathrm{T}$, sabemos que $t \in \mathrm{F}$. Disto, vemos que t é algébrico sobre $k(\mathrm{S})$. Do segundo item da Proposição III.4.6, existe $\mathrm{S}_t \subseteq \mathrm{S}$ finito tal que $t \preceq \mathrm{S}_t$. Isto mostra que $\mathrm{T} \preceq \bigcup_{t \in \mathrm{T}} \mathrm{S}_t$. Disto e de $\mathrm{S} \preceq \mathrm{T}$, obtemos $\mathrm{S} \preceq \bigcup_{t \in \mathrm{T}} \mathrm{S}_t$. Do primeiro item do Lema III.4.7, obtemos $\mathrm{S} = \bigcup_{t \in \mathrm{T}} \mathrm{S}_t$, e portanto, $|\mathrm{T}| \leq |\mathrm{S}|$. Um argumento análogo mostra que $\mathrm{T} = \bigcup_{s \in \mathrm{S}} \mathrm{T}_s$, onde $\mathrm{T}_s \subseteq \mathrm{T}$ é finito para cada $s \in \mathrm{S}$, e portanto $|\mathrm{S}| \leq |\mathrm{T}|$. Da infinitude das duas bases, obtemos $|\mathrm{S}| = |\mathrm{T}|$.

(2) Suponhamos que T seja finita. Vamos provar por indução em $n = |\mathrm{T} - \mathrm{S}|$. Se $n = 0$, então $\mathrm{T} \subseteq \mathrm{S}$. Sabemos que $\mathrm{S} \preceq \mathrm{T}$. Neste caso, segue do primeiro item do Lema III.4.7 que S = T. Suponhamos que o resultado seja válido para n positivo. Existe $t \in \mathrm{T} - \mathrm{S}$. Se valesse $\mathrm{S} \preceq \mathrm{T} - t$, então teríamos $\mathrm{T} \preceq \mathrm{T} - t$, e portanto, $t \preceq \mathrm{T} - t$, o que contradiria T ser k-algebricamente independente em F. Isto mostra que existe $s \in \mathrm{S}$ tal que $s \not\preceq \mathrm{T} - t$. Disto e de $\mathrm{T} - t$ ser k-algebricamente independente em F, segue do segundo item do Lema III.4.7 que $(\mathrm{T} - t) \cup s$ é k-algebricamente independente em F. Temos então $s \preceq \mathrm{T}$ e $s \not\preceq \mathrm{T} - t$. Do quarto item da Proposição III.4.6, obtemos $t \preceq (\mathrm{T} - t) \cup s$. Da arbitrariedade de t em T, obtemos $\mathrm{T} \preceq (\mathrm{T} - t) \cup s$, e portanto, $(\mathrm{T} - t) \cup s$ é uma base de transcendência de $k \subseteq \mathrm{F}$. Temos $|[(\mathrm{T} - t) \cup s] - \mathrm{S}| = n - 1$. Segue da hipótese de indução que $(\mathrm{T} - t) \cup s$ e S são equicardinais, e portanto, T e S são equicardinais. Do Princípio de Indução, obtemos $|\mathrm{S}| = |\mathrm{T}|$. ⊣

[n] O Lema de Zorn (ou de Kuratowski-Zorn) é uma das famosas encarnações do Axioma da Escolha. Uma possível formulação é a seguinte: se toda cadeia em um conjunto parcialmente ordenado admite uma cota superior neste conjunto parcialmente ordenado, então existe um elemento maximal neste conjunto parcialmente ordenado. Vide L. Halbeisen [4] ou K. Hrbáček e T. Jech [7] para discussões mais detalhadas deste princípio maximal e de outras versões do Axioma da Escolha.

O *grau de transcendência* de uma extensão $k \subseteq \mathrm{F}$ é a cardinalidade de uma base de transcendência desta extensão. Extensões de corpos com grau de transcendência finita e positiva dão origem à matroides finitas.

COROLÁRIO III.4.10. Suponhamos que $k \subseteq \mathrm{F}$ seja uma extensão de corpos e que $\mathrm{E} \subseteq \mathrm{F}$ seja um subconjunto finito de F tal que $k \subseteq k(\mathrm{E})$ tenha grau de trancendência finita. Denotemos por $\mathcal{B}$ a coleção das bases de transcendência de $k \subseteq k(\mathrm{E})$.

(1) Se $\mathrm{A}, \mathrm{B} \in \mathcal{B}$ e existe $a \in \mathrm{A} - \mathrm{B}$, então existe $b \in \mathrm{B} - \mathrm{A}$ tal que $(\mathrm{A} - a) \cup b \in \mathcal{B}$.

(2) Dados $\mathrm{S}_1, \mathrm{S}_2 \subseteq \mathrm{E}$ com $\mathrm{S}_1 \subseteq \mathrm{S}_2$, se existem $\mathrm{B}_1, \mathrm{B}_2 \in \mathcal{B}$ tais que $\mathrm{S}_1 \subseteq \mathrm{B}_1$ e $\mathrm{B}_2 \subseteq \mathrm{S}_2$, então existe $\mathrm{B} \in \mathcal{B}$ tal que $\mathrm{S}_1 \subseteq \mathrm{B} \subseteq \mathrm{S}_2$. Esta propriedade é conhecida como *propriedade da base intermediária.*

(3) Definamos $\mathcal{I}$ pondo $\mathrm{I} \in \mathcal{I}$ sse existe $\mathrm{B} \in \mathcal{B}$ tal que $\mathrm{I} \subseteq \mathrm{B}$. O par $(\mathrm{E}, \mathcal{I})$ é uma matroide chamada de *matroide algébrica.*

Demonstração.

(1) Suponhamos que exista $a \in \mathrm{A} - \mathrm{B}$. Se valesse $\mathrm{B} \preceq \mathrm{A} - a$, então teríamos $\mathrm{A} \preceq \mathrm{A} - a$, e portanto, $a \preceq \mathrm{A} - a$, o que contradiria A ser k-algebricamente independente em F. Isto mostra que existe $b \in \mathrm{B}$ tal que $b \not\preceq \mathrm{A} - a$. Disto e de $\mathrm{A} - a$ ser k-algebricamente independente em F, segue do segundo item do Lema III.4.7 que $(\mathrm{A} - a) \cup b$ é k-algebricamente independente em F. Temos então $b \preceq \mathrm{A}$ e $b \not\preceq \mathrm{A} - a$. Do quarto item da Proposição III.4.6, obtemos $a \preceq (\mathrm{A} - a) \cup b$. De $|(\mathrm{A} - a) \cup b| = |\mathrm{A}|$, vemos que $(\mathrm{A} - a) \cup b \in \mathcal{B}$.

(2) Tomemos $\mathrm{B} \in \mathcal{B}$ tal que $\mathrm{S}_1 \subseteq \mathrm{B}$ e tal que B maximize $|\mathrm{B}_2 \cap \mathrm{B}|$. Temos $\mathrm{B} \subseteq \mathrm{S}_2$. De fato, suponhamos que exista $a \in \mathrm{S}_2 - \mathrm{B}$. De $\mathrm{B}_2 \subseteq \mathrm{S}_2$, vemos que $a \in \mathrm{B} - \mathrm{B}_2$. Do primeiro item, segue que existe $b \in \mathrm{B}_2 - \mathrm{B}$ tal que $\mathrm{B}' = (\mathrm{B} - a) \cup b \in \mathcal{B}$. De $\mathrm{S}_1 \subseteq \mathrm{S}_2$, sabemos que $a \notin \mathrm{S}_1$, e assim, $\mathrm{S}_1 \subseteq \mathrm{B}'$. Por outro lado, $|\mathrm{B}_2 \cap \mathrm{B}| < |\mathrm{B}_2 \cap \mathrm{B}'|$, o que contradiz a escolha de B em $\mathcal{B}$. Concluímos que $\mathrm{S}_1 \subseteq \mathrm{B} \subseteq \mathrm{S}_2$.

(3) A coleção $\mathcal{I}$ é não-vazia e hereditária. Provemos que ela possui a propriedade de aumento. Tomemos $\mathrm{I}_1, \mathrm{I}_2 \in \mathcal{I}$ quaisquer tais que $|\mathrm{I}_1| < |\mathrm{I}_2|$. Existem $\mathrm{B}_1, \mathrm{B}_2 \in \mathcal{B}$ tais que $\mathrm{I}_1 \subseteq \mathrm{B}_1$ e $\mathrm{I}_2 \subseteq \mathrm{B}_2$. Tomemos $\mathrm{S} = \mathrm{I}_1 \cup \mathrm{B}_2$. Temos $\mathrm{I}_1 \subseteq \mathrm{B}_1$ e $\mathrm{B}_2 \subseteq \mathrm{S}$. Do segundo item, segue que existe $\mathrm{B} \in \mathcal{B}$ tal que $\mathrm{I}_1 \subseteq \mathrm{B} \subseteq \mathrm{S}$. Disto, obtemos $\mathrm{B} - \mathrm{I}_1 \subseteq \mathrm{B}_2$. Sabemos que $|\mathrm{B}| = |\mathrm{B}_2|$. Temos $|\mathrm{B} - \mathrm{I}_1| + |\mathrm{I}_1| = |\mathrm{B}| = |\mathrm{B}_2| = |\mathrm{B}_2 - \mathrm{I}_2| + |\mathrm{I}_2|$. Disto e de $|\mathrm{I}_1| < |\mathrm{I}_2|$, segue $|\mathrm{B}_2 - \mathrm{I}_2| < |\mathrm{B} - \mathrm{I}_1|$. Temos $\mathrm{I}_2 \cap (\mathrm{B} - \mathrm{I}_1) \neq \emptyset$. De fato, suponhamos que $\mathrm{I}_2 \cap (\mathrm{B} - \mathrm{I}_1) = \emptyset$. Disto, obtemos $|\mathrm{B}_2| \geq |\mathrm{I}_2 \cup (\mathrm{B} - \mathrm{I}_1)| = |\mathrm{I}_2| + |\mathrm{B}| - |\mathrm{I}_1| > |\mathrm{B}|$, o que é uma contradição. Existe $a \in \mathrm{I}_2 \cap (\mathrm{B} - \mathrm{I}_1)$. Temos $\mathrm{I} \cup a \subseteq \mathrm{B}$ e $a \in \mathrm{I}_2 - \mathrm{I}_1$ com $\mathrm{I} \cup a \in \mathcal{I}$. O par $(\mathrm{E}, \mathcal{I})$ é uma matroide. ⊣

Dizemos que uma matroide M de posto r é *algebricamente k-representável* quando existe uma extensão de corpos $k \subseteq \mathrm{F}$ de grau de transcendência r e uma função $g : \mathrm{E}(\mathrm{M}) \longrightarrow \mathrm{F}$ tal que para todo $\mathrm{X} \subseteq \mathrm{E}(\mathrm{M})$ vale $\mathrm{X} \in \mathcal{I}(\mathrm{M})$ sse $|g[\mathrm{X}]| = |\mathrm{X}|$ e $g[\mathrm{X}]$ é k-algebricamente independente em F.

PROPOSIÇÃO III.4.11. [15, Proposição 6.7.10 sec. 6.7] Se uma matroide simples é linearmente k-representável, então ela é algebricamente k-representável.

Demonstração. Suponhamos que M seja uma matroide sobre E = E(M) de posto $r = r(\mathrm{M})$. Se M é linearmente k-representável, então existe $f : \mathrm{E} \longrightarrow \mathrm{V}(r,k)$ tal que para todo $\mathrm{X} \subseteq \mathrm{E}$ vale $\mathrm{X} \in \mathcal{I}(\mathrm{M})$ sse $|f[\mathrm{X}]| = |\mathrm{X}|$ e $f[\mathrm{X}]$ é linearmente independente. Dada uma base $\mathrm{B} = \{ b_1, \ldots, b_r \}$, definamos $v_1 = f(b_1)$, ..., $v_r = f(b_r)$. Tomemos $\Theta = \{ \theta_1, \ldots, \theta_r \}$ um conjunto k-algebricamente independente de r elementos transcendentes sobre k e consideremos a extensão puramente transcendente $\mathrm{F} = k(\theta_1, \ldots, \theta_r)$. Definamos $g : \mathrm{E} \longrightarrow \mathrm{F}$ pondo $\theta_1 = f(b_1)$, ..., $\theta_r = f(b_r)$ de modo que para todo $x \in \mathrm{E} - \mathrm{B}$, se $f(x) = a_1 v_1 + \cdots + a_r v_r$, então $g(x) = a_1\theta_1 + \cdots + a_r\theta_r$. Nas expressões anteriores, a_1, ..., a_r são elementos de k. Se $\mathrm{B}' = \{ b'_1, \ldots, b'_r \}$ é uma base de M, então existe um k-isomorfismo $\alpha : \mathrm{V}(r,k) \longrightarrow \mathrm{V}(r,k)$ tal que $\alpha[f[\mathrm{B}]] = f[\mathrm{B}']$, e portanto, $\alpha[g[\mathrm{B}]] = g[\mathrm{B}']$. Isto mostra que $g[\mathrm{B}']$ é um conjunto k-algebricamente independente de r elementos transcendentes sobre k. Por outro lado, se $\mathrm{C} = \{ c_1, \ldots, c_s \}$ é um circuito de M, então existem escalares a_1, ..., $a_s \in k$ nem todos nulos tais que $a_1 f(c_1) + \cdots + a_s f(c_s) = 0$, e portanto, $a_1 g(c_1) + \cdots + a_s g(c_s) = 0$. Isto mostra que $g[\mathrm{C}]$ é k-algebricamente dependente em F. Concluímos que M é algebricamente k-representável. ⊣

A proposição III.4.11 mostra que a classe das matroides linearmente representáveis está contida na classe das matroides algebricamente representáveis. Isto motiva então o seguinte problema:

PROBLEMA III.4.12. A classe das matroides algebricamente representáveis é definível?

Como observamos na introdução da dissertação, seria muito estranho que tal linguagem pudesse definir a classe maior, mas não a classe menor. Para mostrar que a linguagem $\mathrm{L_I}$ não é capaz de definir a classe das matroides algebricamente representáveis, vamos exibir um conjunto de matroides que atende às hipóteses do Corolário III.3.9. Vejamos um exemplo que será útil para o enunciado da Proposição III.4.14.

EXEMPLO III.4.13. Dado um número primo p, suponhamos que $\mathrm{N}_p \cong \mathrm{M}(\mathrm{B}_p)$, onde B_p é a GF(p)-matriz de tamanho $(p+1) \times (2p+3)$ a seguir:

$$\mathrm{B}_p = \begin{array}{c} \begin{matrix} x_1 & x_2 & \cdots & x_p & x_{p+1} & y_0 & y_1 & y_2 & \cdots & y_p & y_{p+1} \end{matrix} \\ \left[\begin{matrix} 1 & 0 & \cdots & 0 & 0 & 1 & 0 & 1 & \cdots & 1 & 1 \\ 0 & 1 & \cdots & 0 & 0 & 1 & 1 & 0 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & 0 & 0 & 1 & 1 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 1 & 1 & 1 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 1 & 1 & 1 & \cdots & 1 & 0 \end{matrix}\right] \end{array}.$$

Por exemplo, a Matroide de Fano da Figura III.3.3 é a matroide N_2. A matroide N_p é algebricamente GF(p)-representável. De fato, a matroide N_p tem posto $p+1$. Procedemos como na Proposição III.4.11. Suponhamos que x_1, ..., x_p, x_{p+1} sejam $p+1$ transcendentes GF(p)-algebricamente independentes e escrevamos $k = \mathrm{GF}(p)$ e $\mathrm{F} = k(x_1, \ldots, x_{p+1})$. Tomemos $y_0 = x_1 + \cdots + x_{p+1}$ e $y_i = y_0 - x_i$ para cada $i \in \{1, \ldots, p+1\}$. Isto define uma função $g : \mathrm{E}(\mathrm{N}_p) \longrightarrow \mathrm{F}$ tal que para cada $\mathrm{X} \subseteq \mathrm{E}(\mathrm{M})$ vale $\mathrm{X} \in \mathcal{I}(\mathrm{M})$ sse $|g[\mathrm{X}]| = |\mathrm{X}|$ e $g[\mathrm{X}]$ é k-algebricamente independente em F. ⊣

O seguinte resultado provado por Lindström [11] será útil para obter a indefinibilidade da representabilidade algébrica de matroides pela linguagem monádica

de segunda ordem estudada de maneira análoga àquela feita na seção anterior. Vamos assumí-lo sem apresentar sua demonstração, que pode ser encontrada no referido artigo. A prova apresentada por Lindström depende de uma exposição sistemática de derivações[o] em corpos e sob quais condições tais derivações podem ser estendidas.

PROPOSIÇÃO III.4.14. [11, Teorema] A matroide N_p do Exemplo III.4.13 é algebricamente k-representável sse a característica de k é p.

Usando os resultados da Proposição III.4.14 e da Proposição III.4.11, vemos que as matroides N_p são algebricamente k-representáveis sse k tem característica p. Os seguintes resultados também serão úteis para os nossos propósitos e vamos assumí-los sem apresentar suas demonstrações, que podem ser encontradas no referido livro.

PROPOSIÇÃO III.4.15.

(1) [21, Teorema 3 sec. 11.3] A soma direta de matroides algebricamente k-representáveis é algebricamente k-representável.

(2) [21, Teorema 1 sec. 11.3] Se M é algebricamente k-representável e N é um menor de M, então N é algebricamente k-representável.

De posse dos resultados das Proposições III.4.14 e III.4.15, obtemos um conjunto infinito e enumerável de matroides que atende às hipóteses do Corolário III.3.9. Com isso, obtemos o seguinte corolário do Teorema III.3.8, que estende os resultados provados por D. Mayhew, M. Newman e G. Whittle [12] do contexto linear para o contexto algébrico:

COROLÁRIO III.4.16. Não existe $\varphi \in \mathrm{Snt}(\mathrm{L_I})$ tal que $\mathrm{M} \in \mathrm{Mod}(\mathrm{T_I} + \varphi)$ sse $\mathrm{M} \in \mathrm{Mod}(\mathrm{T_I})$ é algebricamente representável.

III.5 UM PROBLEMA DE DECISÃO

Apresentaremos nesta seção um problema de decisão interessante que diz respeito a um tipo especial de amálgama própria de matroides. As referências principais desta seção são J. Oxley [15] e D. Mayhew, M. Newman e G. Whittle [12].

Tomemos $\mathrm{L} \cong \mathrm{U}_{2,5}$. A classe das matroides que tem um menor isomorfo à L é definível pela Proposição III.2.9. Escrevemos $\mathrm{Mod_L}(\mathrm{T_I})$ para abreviar $\mathrm{Mod}(\mathrm{T_I} + \mu_\mathrm{L})$. Do Teorema II.4.9, sabemos que a amálgama própria $\mathrm{M} \oplus_\mathrm{L} \mathrm{N}$ está bem-definida para todas $\mathrm{M}, \mathrm{N} \in \mathrm{Mod_L}(\mathrm{T_I})$ tais que $\mathrm{E(M)} \cap \mathrm{E(N)} = \mathrm{T}$. A linguagem $\mathrm{L_I}$ tem como predicado mais importante o predicado Ind que expressa independência de conjuntos. Um problema interessante é o seguinte problema de decisão:

PROBLEMA III.5.1. Dadas duas matroides $\mathrm{M}, \mathrm{N} \in \mathrm{Mod_L}(\mathrm{T_I})$ e dois conjuntos $\mathrm{X} \subseteq \mathrm{E(M)}$ e $\mathrm{Y} \subseteq \mathrm{E(M)}$, denotemos por c o nome de $\mathrm{X} \cup \mathrm{Y}$ em $\mathrm{L_I}(\mathrm{M} \oplus_\mathrm{L} \mathrm{N})$. Existe um método efetivo para decidir se $\mathrm{M} \oplus_\mathrm{L} \mathrm{N} \models \mathrm{Ind}\, c$?

[o] Lindström parte de representações algébricas e obtém representações lineares sobre o espaço vetorial das derivações para concluir resultados sobre as características dos corpos utilizados. As pessoas que se interessaram por derivações em corpos são convidadas a conferir D. J. Winter [22] para mais informações.

Suponhamos que $M \in \mathrm{Mod}_L(T_I)$. Dado $X \subseteq E(M)$, segue da submodularidade do posto que $r_M(X \cup T) \leq r_M(X - T) + 2$. Definamos:

$$\pi(X) = r_M(X - T) - r_M(X \cup T) + 2.$$

O número natural $\pi(X)$ é chamado de *conectividade local* de $(X - T, T)$. Da submodularidade do posto, temos $0 \leq \pi(X) \leq 2$. A conectividade local será importante para definir a compatibilidade de registros (que definiremos após a demonstração do seguinte lema).

LEMA III.5.2. Suponhamos que $M \in \mathrm{Mod}_L(T_I)$ seja uma matroide com $L \cong U_{2,5}$ e que $I \in \mathcal{I}(M)$. Valem:

(1) Se $\pi(I) = 0$, então $|I \cap T| \leq 2$.

(2) Se $\pi(I) = 1$, então os conjuntos $\alpha = \mathrm{cl}_M(I - T) \cap T$ e $\beta = I \cap T$ são disjuntos e no máximo unitários.

(3) Se $\pi(I) = 2$, então $T \subseteq \mathrm{cl}_M(I - T)$. Neste caso, dizemos que $I - T$ gera T em M.

Demonstração. Suponhamos que $I \in \mathcal{I}(M)$. Provaremos os itens dois e três.

(2) Observemos que se $\pi(I) = 1$, então $|I \cap T| \leq 1$. De fato, se valesse $2 \leq |I \cap T|$, então teríamos

$$\begin{aligned} r_M(I) &= r_M(I \cup T) \\ &= r_M(I - T) - \pi + 2 \\ &= |I - T| + 1 \\ &< |I|, \end{aligned}$$

o que contradiria $I \in \mathcal{I}(M)$. Definamos $\alpha = \mathrm{cl}_M(I - T) \cap T$ e $\beta = I \cap T$. Vale $\alpha \cap \beta = \emptyset$. De fato, se existisse $a \in \alpha \cap \beta$, então existiria $C \in \mathcal{C}(M)$ tal que $a \in C$ e $C \subseteq (I - T) \cup a \subseteq I$, o que contradiria $I \in \mathcal{I}(M)$. Da submodularidade do posto, vemos que:

$$\begin{aligned} r_M(\alpha) &\leq r_M(\mathrm{cl}_M(I - T)) + r_M(T) \\ &\quad - r_M(\mathrm{cl}_M(I - T) \cup T) \\ &= r_M(I - T) + 2 - r_M((I - T) \cup T) \\ &= r_M(I - T) - r_M(I \cup T) + 2 \\ &= \pi(I) \\ &= 1. \end{aligned}$$

Se valesse $2 \leq |\alpha|$, então teríamos $\alpha \subseteq T$ com $r_M(\alpha) = 2$, o que seria uma contradição com $r_M(\alpha) \leq 1$. Disto, segue que $|\alpha| \leq 1$.

(3) Se $\pi(I) = 2$, então $r_M(I - T) = r_M(I \cup T)$. Temos $I - T \subseteq I \cup T$. Da Proposição II.2.16, obtemos $\mathrm{cl}_M(I - T) = \mathrm{cl}_M(I \cup T)$, e assim, $T \subseteq \mathrm{cl}_M(I - T)$. ⊣

Os resultados do Lema III.5.2 serão importantes para motivar as definições a seguir. Tomemos $\Sigma = A \cup \{0, 1, 2\}$, onde o conjunto

$$\begin{aligned} A = \{D, S\} &\cup \{\alpha : \alpha \subseteq T \wedge |\alpha| \leq 2\} \cup \\ &\{(\alpha, \beta) : \alpha, \beta \subseteq T \wedge \alpha \cap \beta = \emptyset \wedge |\alpha|, |\beta| \leq 1\} \end{aligned}$$

é assim definido em virtude do resultado do Lema III.5.2. Vamos aproveitar a ideia de registros das seções anteriores e definir uma nova classe de registros que denominaremos também de registros. Como não usaremos a partir daqui a noção antiga de registros, não haverá confusão neste novo contexto. Para cada número natural positivo m, um (m, L)-*registro* é uma função $\mathrm{R} : \{1, \ldots, m+2\} \times \{1, \ldots, m\} \longrightarrow \Sigma$ tal que a imagem direta de elementos de $\{1, \ldots, m\} \times \{1, \ldots, m\}$ é ou 0 ou 1, a imagem direta de elementos de $\{m+1\} \times \{1, \ldots, m\}$ é um elemento de A e a imagem direta de elementos de $\{m+2\} \times \{1, \ldots, m\}$ é ou 0 ou 1 ou 2. Representamos um (m, L)-registro utilizando um quadro como aquele da Figura III.3.1, no qual rotulamos as colunas e linhas de acordo com o que mostra a mesma figura. O número máximo possível de (m, L)-registros é $2^{m^2} \cdot 3^m \cdot 7^{2m}$. Suponhamos que φ seja uma fórmula de $\mathrm{L_I}$ livre de quantificadores com m variáveis livres x_1, ..., x_m. Dados dois (m, L)-registros R e S, definimos a relação $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\ \varphi)$ de φ-*compatibilidade de* (m, L)-*registros*[p] recursivamente da seguinte forma:

(1) $\mathrm{R} \not\equiv \mathrm{S}\ (\mathrm{comp}\ \bot)$

(2) $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\ \mathrm{Ind}\, x_n)$ sse o fluxograma da Figura III.5.1 retorna a saída "compatível" para as entradas $\omega = \mathrm{R}(m+1, n)$ e $\omega' = \mathrm{S}(m+1, n)$.

(3) $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\ \mathrm{Sng}\, x_n)$ sse $\mathrm{R}(m+2, n) + \mathrm{S}(m+2, n) = 1$, onde $n \in \{1, \ldots, m\}$.

(4) $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\ x_i \sqsubseteq x_j)$ sse $\mathrm{R}(i, j) \cdot \mathrm{S}(i, j) = 1$, onde $i, j \in \{1, \ldots, m\}$.

(5) $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\ \alpha \wedge \beta)$ sse $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\ \alpha)$ e $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\ \beta)$.

(6) $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\ \alpha \vee \beta)$ sse $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\ \alpha)$ ou $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\ \beta)$.

(7) $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\ \alpha \rightarrow \beta)$ sse $\mathrm{R} \not\equiv \mathrm{S}\ (\mathrm{comp}\ \alpha)$ ou $\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\ \beta)$.

Uma matroide empilhada é o que já conhecemos de seções anteriores: uma lista $(\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m)$, na qual $\mathrm{M} \in \mathrm{Mod_L}(\mathrm{T_I})$ e X_1, ..., $\mathrm{X}_m \subseteq \mathrm{E(M)}$. A diferença da noção de matroide empilhada das seções anteriores para a seção atual é a classe à qual pertence a matroide M. Podemos construir (m, L)-registros associados a uma matroide empilhada $(\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m)$ que codificam as informações básicas relevantes para a linguagem $\mathrm{L_I}$ sobre os conjuntos X_1, ..., X_m. Para cada matroide empilhada $(\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m)$, definamos o (m, L)-registro $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!]$ recursivamente da seguinte maneira:

(1) Para $i, j \in \{1, \ldots, m\}$, definimos $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!](i, j) = 1$ sse $\mathrm{X}_i \subseteq \mathrm{X}_j$.

(2) Para $n \in \{1, \ldots, n\}$, definimos:

(2.1) Se $\mathrm{X}_n \notin \mathcal{I}(\mathrm{M})$, então $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!](m+1, n) = \mathrm{D}$.

(2.2) Suponhamos que $\mathrm{X}_n \in \mathcal{I}(\mathrm{M})$. Em virtude do Lema III.5.2, temos três casos para analisar segundo a conectividade local de $(\mathrm{X}_n - \mathrm{T}, \mathrm{T})$:

(2.2.1) Se $\pi(\mathrm{X}_n) = 0$, então $[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!](m+1, n) = \mathrm{X}_n \cap \mathrm{T}$.

[p] Pode valer a pena comparar as duas noções de registros e compatibilidade apresentadas nesta seção e na Seção III.3 a fim de evidenciar as diferenças dessas classes de objetos distintos.

(2.2.2) Se $\pi(X_n) = 1$, então $[\![M, X_1, \ldots, X_m]\!](m+1, n) = (\alpha, \beta)$, onde

$$\alpha = \mathrm{cl}_M(X_n - T) \cap T$$
$$\beta = X_n \cap T.$$

(2.2.3) Se $\pi(X_n) = 2$, então $[\![M, X_1, \ldots, X_m]\!](m+1, n) = S$.

(3) Para $n \in \{1, \ldots, n\}$, definimos:

(3.1) $[\![M, X_1, \ldots, X_m]\!](m+2, n) = 0$ sse $X_n = \emptyset$.

(3.2) $[\![M, X_1, \ldots, X_m]\!](m+2, n) = 1$ sse $|X_n| = 1$.

(3.3) $[\![M, X_1, \ldots, X_m]\!](m+2, n) = 2$ sse $1 < |X_n|$.

O Teorema III.5.3 mostra a corretude do fluxograma da Figura III.5.1, e portanto, existe um método efetivo que responde positivamente o Problema III.5.1. Este resultado é importante, pois permite determinar a independência de conjuntos de amálgamas próprias analisando o seu comportamento local em $L \cong U_{2,5}$.

TEOREMA III.5.3. [12, Parte da Afirmação 6.1.1] Tomemos $M, N \in \mathrm{Mod}_L(T_I)$ tais que $E(M) \cap E(N) = T$ e tomemos também $X_1, \ldots, X_m \subseteq E(M)$ e $Y_1, \ldots, Y_m \subseteq E(N)$. Para cada $i \in \{1, \ldots, m\}$, denotemos por c_i o nome de $X_i \cup Y_i$ em $L_I(M \oplus_L N)$. As seguintes afirmações são equivalentes:

(1) $[\![M, X_1, \ldots, X_m]\!] \equiv [\![N, Y_1, \ldots, Y_m]\!]$ (comp Ind z_n).

(2) $M \oplus_L N \models \frac{c_1, \ldots, c_m}{z_1, \ldots, z_m}$ Ind z_n.

Demonstração. Escrevamos $M_1 = M$, $M_2 = N$ e $U = M \oplus_L N$, tomemos $\omega = [\![M, X_1, \ldots, X_m]\!](m+1, n)$ e $\omega' = [\![N, Y_1, \ldots, Y_m]\!](m+1, n)$ e definamos $Z_1 = X_1 \cup Y_1$, ..., $Z_m = X_m \cup Y_m$. Vamos mostrar que os (m, L)-registros são Ind z_n-compatíveis sse Z_n é independente em U. Seguiremos o fluxograma da Figura III.5.1 analisando cada bloco começando pelo bloco I da mesma Figura:

(I.0) Caso $\omega = D$ ou $\omega' = D$. Neste caso, temos $X_n \notin \mathcal{I}_1$ ou $Y_n \notin \mathcal{I}_2$. Da Figura III.5.1, vemos que (m, L)-registros não são Ind z_n-compatíveis. Do Teorema II.4.13, vemos também que $Z_n = X_n \cup Y_n$ é dependente em U.

(I.1) Caso $\omega \neq D$ e $\omega' \neq D$. Neste caso, temos $X_n \in \mathcal{I}_1$ e $Y_n \in \mathcal{I}_2$ e seguimos para o ramo 1 do bloco I.

Analisamos agora o bloco II da Figura III.5.1:

(II.0) Caso $\omega = S$ ou $\omega' = S$. Sem perda de generalidade, podemos supor que $\omega = S$. Seguimos para o ramo 0 do bloco II. De $\omega = S$, vemos que $X_n - T$ gera T em M_1.

Afirmação 1. Se $X_n - T$ gera T em M_1, então $X_n - T = X_n$.

Demonstração. Suponhamos que $X_n \nsubseteq X_n - T$. Disto, segue que existe $a \in X \cap T$. Como $X_n - T$ gera T, sabemos que $a \in \mathrm{cl}_1(X_n - T)$. Disto, segue que existe um único $C \in \mathcal{C}_1$ tal que $a \in C$ e $C \subseteq (X_n - T) \cup a \subseteq X_n$, o que contradiz $X_n \in \mathcal{I}_1$. ⊣

Da Afirmação 1, segue $X_n - T = X_n$. Disto, obtemos $T \subseteq \mathrm{cl}_1(X_n)$.

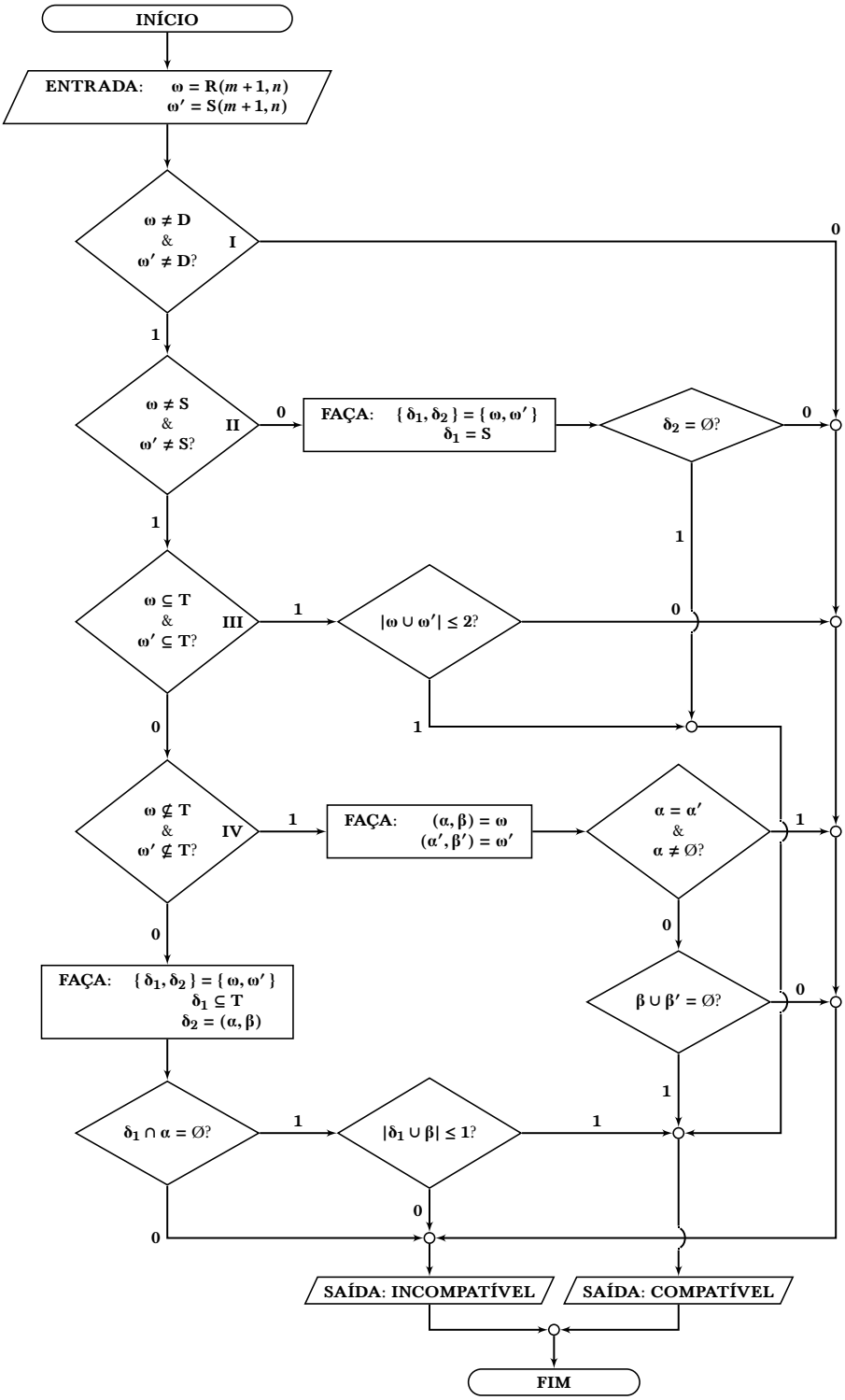

Figura III.5.1: A figura apresenta o fluxograma usado para determinar a compatibilidade de (m, L)-registros para a fórmula atômica que expressa independência.

(i) Se $\omega' \neq \emptyset$, então os (m, L)-registros não são Ind z_n-compatíveis. Se $\omega' \subseteq \mathrm{T}$, então $\omega' = \mathrm{Y}_n \cap \mathrm{T}$. Disto, segue que existe $a \in \mathrm{Y}_n$ tal que $a \in \mathrm{T} \subseteq \mathrm{cl}_1(\mathrm{X}_n - \mathrm{T}) = \mathrm{cl}_1(\mathrm{X}_n)$. Existe um único circuito C de U tal que $a \in \mathrm{C}$ e $\mathrm{C} \subseteq \mathrm{X}_n \cup a \subseteq \mathrm{X}_n \cup \mathrm{Y}_n$. Isto mostra que Z_n é dependente em U. Se $\omega' \nsubseteq \mathrm{T}$, então a conectividade local de $(\mathrm{Y}_n - \mathrm{T}, \mathrm{T})$ é positiva. Disto, segue que $r_2(\mathrm{Y}_n \cup \mathrm{T}) < r_2(\mathrm{Y}_n - \mathrm{T}) + 2$. Temos $\mathrm{Y}_n \cup \mathrm{T} = (\mathrm{Z}_n - \mathrm{E}_1) \cup \mathrm{T}$ e $\mathrm{Y}_n - \mathrm{T} = \mathrm{Z}_n - \mathrm{E}_1$, e portanto, $r_2((\mathrm{Z}_n - \mathrm{E}_1) \cup \mathrm{T}) < r_2(\mathrm{Z}_n - \mathrm{E}_1) + 2$. Do Teorema II.4.13, vemos que Z_n é dependente em U.

(ii) Se $\omega' = \emptyset$, então os (m, L)-registros são Ind z_n-compatíveis. Neste caso, vemos que a conectividade local de $(\mathrm{Y}_n - \mathrm{T}, \mathrm{T})$ é nula. Temos então $r_2(\mathrm{Y}_n \cup \mathrm{T}) = r_2(\mathrm{Y}_n - \mathrm{T}) + 2$ e $\mathrm{Z}_n \cap \mathrm{T} = \emptyset$ e da Afirmação 1, segue $\mathrm{Y}_n - \mathrm{T} = \mathrm{Y}_n$. Disto, obtemos $r_2(\mathrm{Y}_n) + 2 = r_2(\mathrm{Y}_n \cup \mathrm{T})$.

Afirmação 2. Se $r_1(\mathrm{Y}_n - \mathrm{T}) + 2 = r_1(\mathrm{Y}_n \cup \mathrm{T})$, então $\mathrm{cl}_1(\mathrm{Y}_n - \mathrm{T}) \cap \mathrm{T} = \emptyset$.

Demonstração. Da submodularidade do posto, vemos que:

$$\begin{aligned} r_1(\mathrm{cl}_1(\mathrm{Y}_n - \mathrm{T}) \cap \mathrm{T}) &\leq r_1(\mathrm{cl}_1(\mathrm{Y}_n - \mathrm{T})) + r_1(\mathrm{T}) \\ &\quad - r_1(\mathrm{cl}_1(\mathrm{Y}_n - \mathrm{T}) \cup \mathrm{T}) \\ &= r_1(\mathrm{Y}_n - \mathrm{T}) + 2 - r_1((\mathrm{Y}_n - \mathrm{T}) \cup \mathrm{T}) \\ &= r_1(\mathrm{Y}_n - \mathrm{T}) - r_1(\mathrm{Y}_n \cup \mathrm{T}) + 2 \\ &= 0. \end{aligned}$$

⊣

Da Afirmação 2, segue que $\mathrm{cl}_2(\mathrm{Y}_n) \cap \mathrm{T} = \emptyset$. Temos $\mathrm{Y}_n \cup \mathrm{T} = (\mathrm{Z}_n - \mathrm{E}_1) \cup \mathrm{T}$ e $\mathrm{Y}_n - \mathrm{T} = \mathrm{Z}_n - \mathrm{E}_1$. Do Teorema II.4.13, vemos que Z_n é independente em U.

(II.1) Caso $\omega \neq \mathrm{S}$ e $\omega' \neq \mathrm{S}$. Neste caso, seguimos para o ramo 1 do bloco II da Figura III.5.1. Observemos que $\mathrm{X}_n - \mathrm{T}$ não gera T em M e $\mathrm{Y}_n - \mathrm{T}$ não gera T em N.

Analisamos agora o bloco III da Figura III.5.1:

(III.1) Caso $\omega \subseteq \mathrm{T}$ e $\omega' \subseteq \mathrm{T}$. Vemos que $r_1(\mathrm{X}_n - \mathrm{T}) - r_1(\mathrm{X}_n \cup \mathrm{T}) + 2 = 0$ e $r_2(\mathrm{Y}_n - \mathrm{T}) - r_2(\mathrm{Y}_n \cup \mathrm{T}) + 2 = 0$. Segue da Afirmação 2 que $\mathrm{cl}_1(\mathrm{X}_n - \mathrm{T}) \cap \mathrm{T} = \emptyset$ e $\mathrm{cl}_2(\mathrm{Y}_n - \mathrm{T}) \cap \mathrm{T} = \emptyset$.

(i) Suponhamos que $2 < |\omega \cup \omega'|$. Observemos que $\omega \cup \omega'$ é dependente em L. Da Figura III.5.1, vemos que os (m, L)-registros não são Ind z_n-compatíveis. Temos $\mathrm{Z}_n \cap \mathrm{E}_1 = \mathrm{X}_n \cup \omega$ e $\mathrm{Z}_n \cap \mathrm{E}_2 = \mathrm{Y}_n \cup \omega'$. Disto, vemos que $\omega \cup \omega' \subseteq \mathrm{Z}_n$, e portanto, Z_n é dependente em U.

(ii) Suponhamos que $|\omega \cup \omega'| \leq 2$. Da Figura III.5.1, vemos que os (m, L)-registros são Ind z_n-compatíveis. Observemos que $\mathrm{Z}_n \cap \mathrm{T} = \omega \cup \omega'$. De $|\omega \cup \omega'| \leq 2$, vemos que $\omega \cup \omega'$ é independente em L. Temos $\mathrm{X}_n \cup \mathrm{T} = (\mathrm{Z}_n - \mathrm{E}_2) \cup \mathrm{T}$ e $\mathrm{X}_n - \mathrm{T} = \mathrm{Z}_n - \mathrm{E}_2$. Disto e de $r_1(\mathrm{X}_n \cup \mathrm{T}) = r_1(\mathrm{X}_n - \mathrm{T}) + 2$, obtemos $r_1((\mathrm{Z}_n - \mathrm{E}_2) \cup \mathrm{T}) = r_1(\mathrm{Z}_n - \mathrm{E}_2) + 2$. Temos também $\mathrm{Y}_n \cup \mathrm{T} = (\mathrm{Z}_n - \mathrm{E}_1) \cup \mathrm{T}$ e $\mathrm{Y}_n - \mathrm{T} = \mathrm{Z}_n - \mathrm{E}_1$. Disto e de $r_2(\mathrm{Y}_n \cup \mathrm{T}) = r_2(\mathrm{Y}_n - \mathrm{T}) + 2$, obtemos $r_2((\mathrm{Z}_n - \mathrm{E}_1) \cup \mathrm{T}) = r_2(\mathrm{Z}_n - \mathrm{E}_1) + 2$.

Afirmação 3. Se $|\mathrm{Z}_n \cap \mathrm{T}| \leq 2$ com $r_1(\mathrm{X}_n \cup \mathrm{T}) = r_1(\mathrm{X}_n - \mathrm{T}) + 2$ e $r_2(\mathrm{Y}_n \cup \mathrm{T}) = r_2(\mathrm{Y}_n - \mathrm{T}) + 2$, então $\mathrm{Z}_n \cap \mathrm{E}_1 \in \mathcal{I}_1$ e $\mathrm{Z}_n \cap \mathrm{E}_2 \in \mathcal{I}_2$.

Demonstração. Da hipótese $|\mathrm{Z}_n \cap \mathrm{T}| \leq 2$, vemos que $\omega \cup \omega' = \mathrm{Z}_n \cap \mathrm{T} \in \mathcal{I}(\mathrm{L})$. Por hipótese, sabemos que $r_1(\mathrm{X}_n - \mathrm{T}) = r_1(\mathrm{X}_n \cup \mathrm{T}) - 2$. Disto, segue que podemos

estender uma base de $M \mid X_n - T$ para uma base de $M \mid X_n \cup T$ pela adição de dois elementos de T. Isto mostra que $Z_n \cap E_1 = (Z_n - E_2) \cup (Z_n \cap T)$ é independente em $M \mid X_n \cup T$, e portanto, $Z_n \cap E_1 \in \mathcal{I}_1$. Usando um raciocínio análogo, concluímos que $Z_n \cap E_2 \in \mathcal{I}_2$. ⊣

Da Afirmação 3, sabemos que $Z_n \cap E_1 \in \mathcal{I}_1$ e $Z_n \cap E_2 \in \mathcal{I}_2$. Do Teorema II.4.13, vemos que Z_n é independente em U.

(III.0) Caso $\omega \not\subseteq T$ ou $\omega' \not\subseteq T$. Seguimos para o ramo 1 do bloco III.

Analisamos agora o bloco IV da Figura III.5.1:

(IV.1) Caso $\omega \not\subseteq T$ e $\omega' \not\subseteq T$. Neste caso, vemos que as conectividades locais de $(X_n - T, T)$ e $(Y_n - T, T)$ são ambas iguais à 1. Temos $\omega = (\alpha, \beta)$ com $\alpha \cap \beta = \emptyset$ e $|\alpha| \leq 1$ e $|\beta| \leq 1$. Temos também $\omega' = (\alpha', \beta')$ com $\alpha' \cap \beta' = \emptyset$ e $|\alpha'| \leq 1$ e $|\beta'| \leq 1$.

(i) Suponhamos que $\alpha = \alpha'$ e $\alpha \neq \emptyset$. Neste caso, vemos que os (m, L)-registros não são Ind z_n-compatíveis. Existe um único $a \in \alpha = \alpha'$. Disto, vemos que $a \in \mathrm{cl}_1(X_n - T) \cap \mathrm{cl}_2(Y_n - T)$. Do Teorema II.4.13, vemos que Z_n é dependente em U.

(ii) Suponhamos que $\alpha \neq \alpha'$ ou $\alpha = \alpha' = \emptyset$. Suponhamos que $\beta \cup \beta' \neq \emptyset$. Neste caso, vemos que os (m, L)-registros não são Ind z_n-compatíveis. Sabemos que $\beta = X_n \cap T$ e $\beta' = Y_n \cap T$, e assim, $Z_n \cap E_1 = (X_n - T) \cup (\beta \cup \beta')$ e $Z_n \cap E_2 = (Y_n - T) \cup (\beta \cup \beta')$. Se b é o único elemento de $\beta = X_n \cap T$, então $b \in X_n \cap T$ e $b \notin \mathrm{cl}_1(X_n - T)$. De $r_1(X_n \cup T) = r_1(X_n - T) + 1$, vemos que $T \subseteq \mathrm{cl}_1(Z_n \cap E_1)$. Estamos no caso em que $\pi(Y_n) = 1$, e assim, $r_2(Y_n \cup T) = r_2(Y_n - T) + 1$. De $Z_n - E_1 = Y_n - T$, obtemos $r_2((Z_n - E_1) \cup T) < r_2(Z_n - E_1) + 2$. Do Teorema II.4.13, vemos que Z_n é dependente em U. Suponhamos então que $\beta \cup \beta' = \emptyset$. Neste caso, vemos que os (m, L)-registros são Ind z_n-compatíveis e que $Z_n \cap T = \emptyset$. Disto, vemos que $Z_n \cap E_1 = X_n \in \mathcal{I}_1$ e $Z_n \cap E_2 = Y_n \in \mathcal{I}_2$. Como $X_n - T$ não gera T em M_1 e $Y_n - T$ não gera T em M_2, segue que $T \not\subseteq \mathrm{cl}_1(Z_n \cap E_1)$ e $T \not\subseteq \mathrm{cl}_2(Z_n \cap E_2)$. Suponhamos que exista $a \in T$ tal que $a \in \mathrm{cl}_1(Z_n - E_2) \cap \mathrm{cl}_2(Z_n - E_1) = \mathrm{cl}_1(X_n - T) \cap \mathrm{cl}_2(Y_n - T)$. Neste caso, $a \in \alpha \cap \alpha'$, o que contradiz $\alpha \neq \alpha'$ ou $\alpha = \alpha' = \emptyset$. Do Teorema II.4.13, vemos que Z_n é independente em U.

(IV.0) Caso em que apenas uma dentre $\omega \subseteq T$ ou $\omega' \subseteq T$ vale. Podemos supor que $\omega = (\alpha, \beta)$ com $\alpha \cap \beta = \emptyset$ e $|\alpha| \leq 1$ e $|\beta| \leq 1$ e $\omega' \subseteq T$.

(i) Se existe $a \in \omega' \cap \alpha$, então $a \in Y_n \cap T$ e $a \in \mathrm{cl}_1(X_n - T) \cap T$. Neste caso, vemos que os (m, L)-registros não são Ind z_n-compatíveis. De $a \in \mathrm{cl}_1(X_n - T) \cap T$ e $a \in Y_n \cap T$, segue que existe $C \in \mathcal{C}_1$ tal que $a \in C$ e $C \subseteq (X_n - T) \cup a \subseteq X_n \cup (Y_n \cap E_1) = Z_n \cap E_1$. Do Teorema II.4.13, vemos que Z_n é dependente em U.

(ii) Suponhamos que $\omega' \cap \alpha = \emptyset$ e que $\omega' \cup \beta$ tenha dois elementos distintos e e f. Neste caso, vemos que os (m, L)-registros não são Ind z_n-compatíveis. Como $\omega' \cap \alpha = \emptyset$, devemos ter $e \notin \mathrm{cl}_1(X_n - T)$. De $r_1(X_n - T) = r_1(X_n \cup T) - 1$, obtemos $r_1((X_n - T) \cup e) = r_1(X_n \cup T)$, e portanto, $f \in \mathrm{cl}_1((X_n - T) \cup e)$. Disto, vemos que existe $C \in \mathcal{C}_1$ tal que $f \in C$ e $C \subseteq (X_n - T) \cup (e \cup f) \subseteq (X_n - T) \cup (\omega' \cup \beta) = Z_n \cap E_1$. Do Teorema II.4.13, vemos que Z_n é dependente em U. Suponhamos então que $|\omega' \cup \beta| \leq 1$. Neste caso, vemos que os (m, L)-registros são Ind z_n-compatíveis. De $\omega' \cap \alpha = \emptyset$, segue que $(X_n - T) \cup (\omega' \cup \beta) = Z_n \cap E_1$ é independente em M_1 e que $(Y_n - T) \cup (\omega' \cup \beta) = Z_n \cap E_2$ é independente em M_2. Como supomos que

$\omega' \subseteq T$, segue então que $r_2(Y_n - T) - r_2(Y_n \cup T) + 2 = 0$. Da Afirmação 2, vemos que $\mathrm{cl}_2(Y_n - T) \cap T = \emptyset$. Sabemos que $|\omega' \cup \beta| \leq 1$, e assim, $T \not\subseteq \mathrm{cl}_2(Z_n \cap E_2)$. Do Teorema II.4.13, vemos que Z_n é independente em U. ⊣

Tomemos $M, N \in \mathrm{Mod}_L(T_I)$ tais que $E(M) \cap E(N) = T$. Uma pergunta interessante é a seguinte: é possível obter um resultado semelhante ao do teorema anterior para fórmulas atômicas da forma $z_i \sqsubseteq z_j$? Infelizmente, um resultado geral como aquele do teorema anterior não pode ser alcançado para este tipo de fórmula caso consideremos conjuntos arbitrários. O Exemplo III.5.4 mostra como é possível obter um contra-exemplo. Suponhamos que $X_1, \ldots, X_m \subseteq E(M)$ e $Y_1, \ldots, Y_m \subseteq E(N)$. A afirmação $[\![M, X_1, \ldots, X_m]\!] \equiv [\![N, Y_1, \ldots, Y_m]\!]$ $(\mathrm{comp}\, z_i \sqsubseteq z_j)$ sempre implica em $M \oplus_L N \models c_{X_i \cup Y_i} \sqsubseteq c_{X_j \cup Y_j}$, e assim, o problema está localizado na recíproca. Para que $M \oplus_L N \models c_{X_i \cup Y_i} \sqsubseteq c_{X_j \cup Y_j}$ implique em $[\![M, X_1, \ldots, X_m]\!] \equiv [\![N, Y_1, \ldots, Y_m]\!]$ $(\mathrm{comp}\, z_i \sqsubseteq z_j)$ é preciso supor como hipótese adicional que $X_i \cap Y_j \subseteq X_j$ e $X_j \cap Y_i \subseteq Y_j$ e isto impede uma formulação geral.

EXEMPLO III.5.4. Suponhamos que F seja um corpo, que $3 \leq s$ seja um número inteiro e que $a \in F^\times$ seja tal que $2s(s-1) < \mathrm{ord}(\alpha)$. Vimos na Seção II.5 que a matroide $U = M_\Gamma(s, \alpha) \oplus_L M_\Delta(s, \alpha)$ é isomorfa à matroide de ganho obtida do grafo de ganho da Figura II.5.6. Escrevamos $M = M_\Gamma(s, \alpha)$ e $N = M_\Delta(s, \alpha)$. Tomemos os conjuntos $X_1 = \{a_2, \ldots, a_s, b\} \subseteq E(M)$ e $Y_1 = \{a, b_1, \ldots, b_{2t-1}\} \subseteq E(N)$. Os conjuntos $X_2 = \{a, a_2, \ldots, a_s\} \subseteq E(M)$ e $Y_2 = \{b_1, \ldots, b_{2t-1}, b\} \subseteq E(N)$ são tais que $X_1 \cup Y_1 = X_2 \cup X_2$, e portanto, $U \models c_{X_1 \cup Y_1} \sqsubseteq c_{X_2 \cup Y_2}$. Por outro lado, temos $X_1 \not\subseteq X_2$ e $Y_1 \not\subseteq Y_2$, e assim, $[\![M, X_1, X_2]\!](1, 2) = 0$ e $[\![N, Y_1, Y_2]\!](1, 2) = 0$. Disto, obtemos $[\![M, X_1, X_2]\!] \not\equiv [\![N, Y_1, Y_2]\!]$ $(\mathrm{comp}\, a_1 \sqsubseteq a_2)$. ⊣⊢

III.6 TRADUÇÕES E CRIPTOMORFISMOS

Vimos nas seções anteriores que a linguagem L_I não é capaz de expressar a representabilidade de matroides, seja tal representabilidade linear ou algébrica. Esta seção lida com um tópico que não foi abordado por D. Mayhew, M. Newman e G. Whittle [12], mas que se mostrou interessante durante os estudos para a escrita desta dissertação, pois matroides podem ser axiomatizadas de várias maneiras diferentes (Vide Seção II.2 para ver algumas delas). O seguinte problema resume o que se mostrou interessante:

PROBLEMA III.6.1. Tal incapacidade de expressar certa propriedade sobre matroides é uma característica exclusiva da linguagem L_I?

Vamos mostrar nesta seção que a resposta para o Problema III.6.1 é negativa. Para isto, vamos apresentar uma linguagem que permitirá evidenciar como as matroides impõem restrições nas linguagens formais que expressam seus axiomas. A linguagem L_C é a linguagem cujo alfabeto Λ_C é obtido do alfabeto Λ_I pela substituição do símbolo de predicado monádico Ind pelo símbolo de predicado monádico Crc. As regras de formação para L_C são as mesmas de L_I com exceção da regra que forma fórmulas atômicas da forma $\mathrm{Ind}\, t$, que é substituída por uma regra que forma fórmulas atômicas da forma $\mathrm{Crc}\, t$. Os conceitos sintáticos das linguagens são todos preservados, desde que não façam referência ao símbolo Ind. Parte dos conceitos semânticos também são preservados, mas é necessário analisá-los com mais cuidado. Como vimos na Seção III.2, as estruturas da linguagem L_I são pares $N = (E(N), \mathcal{I}(N))$, nos quais as coleções $\mathcal{I}(N)$ interpretam o símbolo

de predicado Ind segundo as regras apresentadas. As estruturas da linguagem L_C são pares $M = (E(M), \mathcal{C}(M))$, nos quais as coleções $\mathcal{C}(M)$ interpretam o símbolo de predicado Crc segundo a seguinte regra:

$$M[\mathrm{Crc}\, c] = 1 \text{ sse } c^M \in \mathcal{C}(M).$$

EXEMPLO III.6.2 (Expressividade). Podemos expressar certas propriedades na linguagem L_C assim como foi feito para a linguagem L_I no Exemplo III.2.2. As fórmulas que não dependem dos símbolos Ind e Crc são preservadas. Fórmulas interessantes são as seguintes:

(1) Podemos expressar em L_C a noção de que o conjunto vazio não é um circuito pela fórmula

$$\mathrm{Non}\, y = \forall x(\mathrm{Crc}\, y \to \neg y \sqsubseteq x).$$

(2) Podemos expressar em L_C a noção de que circuitos formam uma anticadeia pela fórmula

$$\mathrm{Ant}\, xy = \mathrm{Crc}\, x \wedge \mathrm{Crc}\, y \wedge x \sqsubseteq y \to y \sqsubseteq x.$$

(3) Podemos expressar em L_C a propriedade de eliminação de circuitos pela formula

$$\begin{aligned}\mathrm{Eli}\, xy = {} & \mathrm{Crc}\, x \wedge \mathrm{Crc}\, y \wedge \neg x \doteq y \wedge \\ & \exists x_1 \exists x_2(\mathrm{Sng}\, x_1 \wedge x_1 \sqsubseteq x_2 \wedge \mathrm{Int}_2\, xyx_2 \to \\ & \exists x_3 \exists x_4 \exists x_5(\mathrm{Crc}\, x_3 \wedge \mathrm{Uni}_2\, xyx_4 \wedge \mathrm{Dif}\, x_4 x_1 x_5 \wedge x_3 \sqsubseteq x_5)).\end{aligned}$$ ⊣

Vimos na Seção III.2 que a Teoria de Matroides na linguagem L_I é o fecho por consequências lógicas do conjunto finito de axiomas $T_I \subseteq \mathrm{Snt}(L_I)$. A Teoria de Matroides na linguagem L_C é o fecho por consequências lógicas do conjunto finito de axiomas $T_C \subseteq \mathrm{Snt}(L_C)$ cujos elementos são as sentenças $\forall x\, \mathrm{Non}\, x$, $\forall x \forall y\, \mathrm{Ant}\, xy$ e $\forall x \forall y\, \mathrm{Eli}\, xy$ obtidas das fórmulas apresentadas no Exemplo III.6.2. A Proposição III.6.3 segue do que foi discutido na Seção II.2.

PROPOSIÇÃO III.6.3. Para toda $M \in \mathrm{Mod}(T_I)$ existe uma única $M^C \in \mathrm{Mod}(T_C)$ tal que $\mathcal{C}(M^C)$ é a coleção dos circuitos de M. Para toda $N \in \mathrm{Mod}(T_C)$ existe uma única $N^I \in \mathrm{Mod}(T_I)$ tal que $\mathcal{I}(N^I)$ é a coleção dos conjuntos independentes de N.

Agora, estamos prontos para construir as traduções entre as linguagens L_I e L_C. A *tradução de* L_I *para* L_C é a função $-^C : \mathrm{Frm}(L_I) \longrightarrow \mathrm{Frm}(L_C)$ definida recursivamente da seguinte forma:

(1) Primeiro, definimos a tradução de fórmulas iniciais:

(1.1) Se $\varphi = \bot$, então $\varphi^C = \bot$.

(1.2) Se $\varphi = \mathrm{Sng}\, t$, então $\varphi^C = \mathrm{Sng}\, t$.

(1.3) Se $\varphi = s \sqsubseteq t$, então $\varphi^C = s \sqsubseteq t$.

(1.4) Se $\varphi = \mathrm{Ind}\, t$, então $\varphi^C = \forall x(x \sqsubseteq t \to \neg\, \mathrm{Crc}\, x)$.[q]

(2) Uma vez definidas as traduções para fórmulas iniciais, definimos as traduções das fórmulas mais complexas:

(2.1) Se $\varphi = \alpha \wedge \beta$, então $\varphi^C = \alpha^C \wedge \beta^C$.

(2.2) Se $\varphi = \alpha \vee \beta$, então $\varphi^C = \alpha^C \vee \beta^C$.

[q]Em outras palavras: um conjunto é independente quando ele não contém circuitos.

(2.3) Se $\varphi = \alpha \to \beta$, então $\varphi^{C} = \alpha^{C} \to \beta^{C}$.

(2.4) Se $\varphi = \exists x \psi(x)$, então $\varphi^{C} = \exists x \psi(x)^{C}$.

(2.5) Se $\varphi = \forall x \psi(x)$, então $\varphi^{C} = \forall x \psi(x)^{C}$.

Esta tradução permite obter de maneira sistemática fórmulas na linguagem L_C partindo de fórmulas na linguagem L_I. É natural neste ponto pensar como tal noção de tradução se relaciona com os conceitos de verdade formal estudados. O seguinte lema faz esta conexão.

LEMA III.6.4. Dada $M \in \mathrm{Mod}(T_I)$, formemos as linguagens $L_I(M)$ e $L_C(M^C)$. Para cada $\varphi \in \mathrm{Snt}(L_I(M))$, existe $\varphi^C \in \mathrm{Snt}(L_C(M^C))$ tal que $M \models \varphi$ sse $M^C \models \varphi^C$.

Demonstração. Se φ é atômica e sem ocorrências do símbolo de predicado Ind, então vale $M \models \varphi$ sse $M^C \models \varphi^I$. Se $\varphi = \mathrm{Ind}\, c$, então $M \models \varphi$ sse $c^M \in \mathcal{I}(M)$ sse c^M não contém circuitos sse dado $X \subseteq E(M)$ se $X \subseteq c^M$, então $X \notin \mathcal{C}(M)$ sse $M^C \models \forall x(x \sqsubseteq c \to \neg\, \mathrm{Crc}\, x)$ sse $M^C \models \varphi^C$. O restante da demonstração segue por indução no comprimento das sentenças. ⊣

Quando estudamos a Teoria de Matroides na Seção II.2, vimos que existem traduções de conceitos em ambas direções, e assim, podemos também apresentar a tradução oposta da tradução de L_I para L_C. A *tradução de* L_C *para* L_I é a função $-^I : \mathrm{Frm}(L_C) \longrightarrow \mathrm{Frm}(L_I)$ definida recursivamente da seguinte forma:

(1) Primeiro, definimos a tradução de fórmulas iniciais:

(1.1) Se $\varphi = \bot$, então $\varphi^I = \bot$.

(1.2) Se $\varphi = \mathrm{Sng}\, t$, então $\varphi^I = \mathrm{Sng}\, t$.

(1.3) Se $\varphi = s \sqsubseteq t$, então $\varphi^I = s \sqsubseteq t$.

(1.4) Se $\varphi = \mathrm{Crc}\, t$, então $\varphi^I = \neg\, \mathrm{Ind}\, t \wedge \forall x(\neg\, \mathrm{Ind}\, x \wedge x \sqsubseteq t \to t \sqsubseteq x)$.[r]

(2) Uma vez definidas as traduções para fórmulas iniciais, definimos as traduções das fórmulas mais complexas:

(2.1) Se $\varphi = \alpha \wedge \beta$, então $\varphi^I = \alpha^I \wedge \beta^I$.

(2.2) Se $\varphi = \alpha \vee \beta$, então $\varphi^I = \alpha^I \vee \beta^I$.

(2.3) Se $\varphi = \alpha \to \beta$, então $\varphi^I = \alpha^I \to \beta^I$.

(2.4) Se $\varphi = \exists x \psi(x)$, então $\varphi^I = \exists x \psi(x)^I$.

(2.5) Se $\varphi = \forall x \psi(x)$, então $\varphi^I = \forall x \psi(x)^I$.

Esta tradução permite obter de maneira sistemática fórmulas na linguagem L_I partindo de fórmulas na linguagem L_C. É natural neste ponto pensar como tal noção de tradução se relaciona com os conceitos de verdade formal estudados. O seguinte lema faz esta conexão.

LEMA III.6.5. Dada $M \in \mathrm{Mod}(T_C)$, formemos as linguagens $L_C(M)$ e $L_I(M^I)$. Para cada $\varphi \in \mathrm{Snt}(L_C(M))$, existe $\varphi^I \in \mathrm{Snt}(L_I(M^I))$ tal que $M \models \varphi$ sse $M^I \models \varphi^I$.

[r] Em outras palavras: um conjunto é um circuito quando ele é um conjunto dependente minimal.

Demonstração. Se φ é atômica e sem ocorrências do símbolo de predicado Crc, então vale $M \models \varphi$ sse $M^I \models \varphi^I$. Se $\varphi = \mathrm{Crc}\, c$, então $M \models \varphi$ sse $c^M \in \mathcal{C}(M)$ sse c^M não é independente e toda parte própria de c^M é independente sse $c^M \notin \mathcal{I}(M^I)$ e para todo $X \subseteq E(M)$ se $X \notin \mathcal{I}(M^I)$ e $X \subseteq c^M$, então $c^M \subseteq X$ sse $M^I \models \neg\, \mathrm{Ind}\, c \wedge \forall x(\neg\, \mathrm{Ind}\, x \wedge x \sqsubseteq c \rightarrow c \sqsubseteq x)$ sse $M^I \models \varphi^I$. O restante da demonstração segue por indução no comprimento das sentenças. ⊣

O Lema III.6.5 mostra que as traduções de L_C para L_I e de L_I para L_C preservam satisfabilidade de sentenças. Como consequência disto, obtemos o Teorema III.6.6 que mostra que as linguagens L_C e L_I tem o mesmo poder de expressão de conceitos relacionados à Teoria de Matroides.

TEOREMA III.6.6 (Criptomorfismo). Suponhamos que P seja uma propriedade pertinente às matroides. A classe de matroides que possuem a propriedade P é definível em L_I sse tal classe é definível em L_C.

Demonstração. Suponhamos que exista uma sentença $\varphi \in \mathrm{Snt}(L_C)$ tal que para toda $N \in \mathrm{Mod}(T_C)$, tenhamos $N \models \varphi$ sse N possui a propriedade P. Dada $M \in \mathrm{Mod}(T_I)$, suponhamos que M possua a propriedade P. Da Proposição III.6.3, existe uma única $M^C \in \mathrm{Mod}(T_C)$. Da construção de M^C, sabemos que M^C possui a propriedade P sse M possui a propriedade P. Disto, segue $M^C \models \varphi$ e do Lema III.6.5, obtemos $M \models \varphi^I$. Vemos assim que $\varphi^I \in \mathrm{Snt}(L_I)$ é tal que para toda $M \in \mathrm{Mod}(T_I)$ vale $M \models \varphi^I$ sse M possui a propriedade P. A volta é análoga. ⊣

Segue do Teorema III.6.6 que a linguagem L_C também não é capaz de expressar as representabilidades linear e algébrica de matroides. Isto pode ser generalizado naturalmente: qualquer linguagem formal capaz de expressar as representablidades linear ou algébrica de matroides não pode ser traduzida para L_I (ou para L_C) com preservação de satisfabilidade de sentenças.

LISTA DE SÍMBOLOS

SEÇÃO II.1

C_m	Grafo ciclo de m vértices. 18
$E(G)$	Conjunto de arestas de G. 17
$G[U]$	Subgrafo de G induzido por U. 19
$G \mid F$	Subgrafo de G restrito a F. 19
$G \cong H$	G e H são isomorfos. 17
$H \sqsubseteq G$	H é subgrafo de G. 17
K_m	Grafo completo de m vértices. 18
$\mathbb{N}$	Conjunto dos números naturais. 18
P_m	Grafo caminho de m vértices. 18
$V(G)$	Conjunto de vértices de G. 17
$W(u, v)$	(u, v)-passeio. 19
Λ_G	Função de incidência de G. 17

SEÇÃO II.2

2^E	Conjunto das partes de E. 19
$\mathcal{B}(M)$	Coleção das bases de M. 20
$\mathcal{C}(M)$	Coleção dos circuitos de M. 20
$E(M)$	Conjunto subjacente M. 19
$\mathcal{I}(M)$	Coleção dos conjuntos independentes de M. 19
$L \cong M$	L e M são isomorfas. 20
$M(A)$	Matroide linear. 20
$M(G)$	Matroide gráfica. 23
M^*	Matroide dual de M. 28
$M \mid X$	Restrição de M a X. 23
$U_{r,m}$	Matroide uniforme. 23
$V(m, F)$	Espaço vetorial de dimensão m sobre o corpo F. 20
cl_M	Operador de fecho de M. 25
$r(M)$	Posto de M. 23
r_M	Função posto de M. 23

SEÇÃO II.3

$GF(q)$	Corpo finito de q elementos. 29
M / X	Contração de X em M. 30
$M \setminus X$	Deleção de X em M. 30
$M \setminus X / Y$	Menor de M. 31
$M \preceq N$	Existe um M-menor de N. 31

SEÇÃO II.4

$\mathcal{F}(U)$	Coleção dos flats de U. 35
$\mathcal{L}(M_1, M_2)$	Coleção dos $X \subseteq E$ tais que $X \cap E_i \in \mathcal{F}(M_i)$. 35
$M_1 \oplus_L M_2$	Amálgama própria de M_1 e M_2. 35

SEÇÃO II.5

D_Φ	Matriz de incidência de (G, Φ). 46
$F^\times$	Grupo multiplicativo do corpo F. 46
$\mathcal{L}(G)$	Coleção linear de circuitos de G. 44
$M(\Phi)$	Matroide de ganho. 46
$M_\Gamma(s, \alpha)$	Matroide de ganho do grafo de ganho $\Gamma(F, s, \alpha)$. 48
$M_\Delta(t, \beta)$	Matroide de ganho do grafo de ganho $\Delta(F, t, \beta)$. 48
W^{-1}	Percurso oposto de W. 43
W_σ	Permutação cíclica do percurso W. 43
$\mathrm{ord}(\alpha)$	Ordem de α. 46
$\triangle$	Diferença simétrica de conjuntos. 44
Δ_G	Orientação de G. 42
Δ_G^-	Orientação oposta de Δ_G. 42
$\Phi(W)$	Ganho do percurso W. 43

SEÇÃO III.1

$\wedge$	Conectivo lógico de conjunção. 57
$\vee$	Conectivo lógico de disjunção. 57
$\neg$	Conectivo lógico de negação. 61
Ind	Símbolo de predicado de independência. 57
L_I	Linguagem monádica de segunda ordem para Teoria de Matroides que lida com independência como noção primitiva. 57
Sng	Símbolo de predicado de unitariedade. 57
$\frac{t_1,\ldots,t_m}{x_1,\ldots,x_m}s$	Substituição de $x_1, \ldots, x_m$ por $t_1, \ldots, t_m$ em s. 62
$\frac{t_1,\ldots,t_m}{x_1,\ldots,x_m}\varphi$	Substituição de $x_1, \ldots, x_m$ por $t_1, \ldots, t_m$ em φ. 62
$\rightarrow$	Conectivo lógico de implicação (condicional material). 57
$\leftrightarrow$	Conectivo lógico de equivalência material. 61
$\forall$	Quantificador lógico universal. 58
$\exists$	Quantificador lógico existencial. 58
$\sqsubseteq$	Símbolo de predicado de continência (ou inclusão). 57
$\vdash \varphi$	φ é um teorema. 67
$\bot$	Conectivo lógico de falsidade. 57
$\Gamma \Rightarrow \Delta$	Sequente. 62
Λ_I	Alfabeto da linguagem L_I. 57
$\Lambda_I^\star$	Fecho de Kleene de Λ_I. 58

SEÇÃO III.2

$\_^M$	Interpretação de constantes. 76
Base z	z é maximal em $\mathcal{I}(M)$. 78
Cst(L)	Conjunto das constantes de L. 76
Dif $z_1 z_2 z$	z é a diferença de z_1 e z_2. 78
Exc xy	Fórmula que expressa a propriedade de aumento em L_I. 78
Her xy	Fórmula que expressa hereditariedade em L_I. 78
$\mathrm{Int}_n\, z_1 \cdots z_n z_{n+1}$	z_{n+1} é a interseção de $z_1, \ldots, z_n$. 78
$L_I(M)$	Linguagem da estrutura M. 76
$M \equiv N$	Relação de equivalência elementar de matroides. 81
$M \models T$	M satisfaz o conjunto de sentenças T. 80

$\mathrm{M}[-]$	Avaliação de sentenças. 76
$\mathrm{Mod}(\mathrm{T_I})$	Classe dos modelos de $\mathrm{T_I}$. 81
$\mathrm{M} \models \varphi$	M satisfaz a sentença φ. 77
$\mathrm{Snt}(\mathrm{L})$	Conjunto das sentenças de L. 76
$\mathrm{T} \vdash \varphi$	φ é um teorema de T. 80
$\mathrm{T} \models \varphi$	T acarreta φ. 80
$\mathrm{T_I}$	Conjunto dos axiomas da Teoria de Matroides em $\mathrm{L_I}$. 81
$\mathrm{Uni}_n\, z_1 \cdots z_n z_{n+1}$	z_{n+1} é a união de $z_1, \ldots, z_n$. 78
c_{X}	Nome do conjunto X. 76
$\doteq$	Internalização da igualdade na linguagem $\mathrm{L_I}$. 78
$\models \varphi$	φ é válida. 77

SEÇÃO III.3

$(\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m)$	Matroide empilhada. 84
$[\![\mathrm{M}]\!]_m$	m-árvore de M. 89
$\mathrm{M} \equiv_m \mathrm{N}$	Relação de m-equivalência de matroides. 83
$\mathrm{M} \#_m \mathrm{N}$	Relação de apartness de matroides. 83
$[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_k]\!]_n$	n-árvore de $(\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_k)$. 87
$[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!]$	m-registro de $(\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m)$. 84
$\mathrm{Mod}(\mathrm{T_I} + \mathrm{U})$	Classe das matroides que são modelos de U. 82
$\mathrm{M} \simeq_m \mathrm{N}$	M e N têm as mesmas m-árvores. 89
$\mathrm{M} \oplus \mathrm{N}$	Soma direta de M e N. 83
$\mathrm{R} \equiv \mathrm{S}\ (\mathrm{comp}\, \varphi)$	Relação de φ-compatibilidade de m-registros. 84
$\langle\rangle$	Lista vazia. 89

SEÇÃO III.4

$(\mathrm{F} : k)$	Grau da extensão $k \subseteq \mathrm{F}$. 94
$\mathrm{S} \preceq \mathrm{T}$	S é k-algebricamente dependente sobre T em F. 96
$a \preceq \mathrm{S}$	a é k-algebricamente dependente sobre S em F. 96
$k(\mathrm{S})$	Menor subcorpo de F gerado por S que contém k. 94
$k(s_1, \ldots, s_m)$	Vide $k(\mathrm{S})$ para $\mathrm{S} = \{ s_1, \ldots, s_m \}$. 94
$k[\mathrm{S}]$	Menor subdomínio de F gerado por S que contém k. 94
$k[s_1, \ldots, s_m]$	Vide $k[\mathrm{S}]$ para $\mathrm{S} = \{ s_1, \ldots, s_m \}$. 94
$k\langle \mathrm{S} \rangle$	Menor subespaço de F gerado por S que contém k. 94
$k\langle s_1, \ldots, s_m \rangle$	Vide $k\langle \mathrm{S} \rangle$ para $\mathrm{S} = \{ s_1, \ldots, s_m \}$. 94
$\aleph_0$	Cardinalidade do conjunto $\mathbb{N}$. 94

SEÇÃO III.5

$[\![\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m]\!]$	(m, L)-registro de $(\mathrm{M}, \mathrm{X}_1, \ldots, \mathrm{X}_m)$. 104
$\mathrm{Mod}_{\mathrm{L}}(\mathrm{T_I})$	Classe das matroides que tem um L-menor. 102
$\pi(\mathrm{X})$	Conectividade local de $(\mathrm{X} - \mathrm{T}, \mathrm{T})$. 103

SEÇÃO III.6

$-^{\mathrm{C}}$	Tradução de $\mathrm{L_I}$ para $\mathrm{L_C}$. 110
$-^{\mathrm{I}}$	Tradução de $\mathrm{L_C}$ para $\mathrm{L_I}$. 111
$\mathrm{Ant}\, xy$	Fórmula que expressa em $\mathrm{L_C}$ que circuitos formam uma anticadeia. 110

Crc	Símbolo de predicado de dependência minimal. 109
Eli xy	Fórmula que expressa a propriedade de eliminação de circuitos em L_C. 110
L_C	Linguagem monádica de segunda ordem para Teoria de Matroides que lida com dependência minimal como noção primitiva. 109
Non y	Fórmula que expressa em L_C que o conjunto vazio não é um circuito. 110
T_C	Conjunto dos axiomas da Teoria de Matroides em L_C. 110
Λ_C	Alfabeto da linguagem L_C. 109

REFERÊNCIAS

[1] Brylawski, T., H. Crapo, U. Faigle, J. P. Kung, H. Q. Nguyen, G. Nicoletti, J. Oxley, and N. White
1986. *Theory of Matroids*, Encyclopedia of Mathematics and its Applications. Cambridge University Press.

[2] Diestel, R.
2017. *Graph Theory*, 5th edition. Springer Publishing Company, Incorporated.

[3] Gordon, G. and J. McNulty
2012. *Matroids: A Geometric Introduction.* Cambridge University Press.

[4] Halbeisen, L.
2011. *Combinatorial Set Theory: With a Gentle Introduction to Forcing*, Springer Monographs in Mathematics. Springer London.

[5] Halbeisen, L. and R. Krapf
2020. *Gödel's Theorems and Zermelo's Axioms: A Firm Foundation of Mathematics.*

[6] Hliněný, P.
2003. On matroid properties definable in the mso logic. In *Mathematical Foundations of Computer Science 2003*, B. Rovan and P. Vojtáš, eds., Pp. 470–479, Berlin, Heidelberg. Springer Berlin Heidelberg.

[7] Hrbacek, K. and T. Jech
1999. *Introduction to Set Theory, Third Edition, Revised and Expanded*, Chapman & Hall/CRC Pure and Applied Mathematics. Taylor & Francis.

[8] Kozen, D.
2007. *Automata and Computability*, Undergraduate Texts in Computer Science. Springer New York.

[9] Kung, J. P.
1986. *A Source Book in Matroid Theory.*

[10] Libkin, L.
2004. *Elements of Finite Model Theory.* Springer.

[11] Lindström, B.
1985. On the algebraic characteristic set for a class of matroids. *Proceedings of the American Mathematical Society*, 95(1):147–151.

[12] Mayhew, D., M. Newman, and G. Whittle
2017. Yes, the "missing axiom"of matroid theory is lost forever.

[13] Negri, S., J. von Plato, and A. Ranta
2001. *Structural Proof Theory.* Cambridge University Press.

[14] Nishimura, H. and S. Kuroda
2009. *A Lost Mathematician, Takeo Nakasawa: The Forgotten Father of Matroid Theory.*

[15] Oxley, J. G.
1992. *Matroid theory.* Oxford: Oxford University Press.

[16] Pervin, W. and W. Pervin
1964. *Foundations of General Topology*, Academic Press textbooks in mathematics. Academic Press.

[17] Shoenfield, J. R.
1967. *Mathematical Logic.* Reading, Mass., Addison-Wesley Pub. Co.

[18] Takeuti, G.
2013. *Proof Theory*, Dover books on mathematics. Dover Publications, Incorporated.

[19] Troelstra, A. S. and H. Schwichtenberg
2000. *Basic Proof Theory*, Cambridge Tracts in Theoretical Computer Science, 2 edition. Cambridge University Press.

[20] van Dalen, D.
2013. *Logic and Structure*, Universitext. Springer Berlin Heidelberg.

[21] Welsh, D. and L. M. Society
1976. *Matroid Theory*, L.M.S. monographs. Academic Press.

[22] Winter, D., D. Winter, and W. David
1974. *The Structure of Fields*, Graduate Texts in Mathematics. Springer New York.

[23] Zaslavsky, T.
1989. Biased graphs. i. bias, balance, and gains. *Journal of Combinatorial Theory, Series B*, 47(1):32–52.

[24] Zaslavsky, T.
1991. Biased graphs. ii. the three matroids. *Journal of Combinatorial Theory, Series B*, 51(1):46–72.

[25] Zaslavsky, T.
2003. Biased graphs iv: Geometrical realizations. *Journal of Combinatorial Theory, Series B*, 89(2):231–297.