Multiplicadores algébricos de validade lógica

Mauricio Simões Camilo Hernandes

DISSERTAÇÃO APRESENTADA
AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA
OBTENÇÃO DO TÍTULO
DE
MESTRE EM CIÊNCIAS

Programa: Matemática

Orientador: Prof. Dr. Marcelo Finger

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro da CNPq

São Paulo, março de 2010

Agradecimentos

Gostaria de começar agradecendo à minha minha família; minha mãe, Célia, meu Pai, Mauricio, sua mulher Mila, meus irmãos Marjorie e Demitri; a maior e melhor agência de fomento à pesquisa que já me deu apoio, sem eles eu não estaria aqui e sem eles eu não irei além. Agradeço à minha veterana Antonieta por envelhecer comigo todos esses anos fazendo-me sentir uma pessoa normal a cada amargura e por estar ao meu lado me ajudando sempre que meus prazos estão para estourar. Agradeço à Beatriz por me fazer sentir uma pessoa especial a cada momento. Agradeço ao meu orientador Marcelo Finger, tanto pelas horas de ausência, quanto pelas horas de conselho, termino este trabalho tendo certeza que eu não poderia ter escolhido melhor. Agradeço aos professores de lógica e fundamentos da matemática do meu instituto em especial ao Hugo Mariano e Ricardo Bianconi, sempre resolvendo minhas dúvidas sobre lógica e ao Professor Antônio de Pádua, sempre resolvendo minhas dúvidas sobre o universo e tudo mais.

Quero agradecer ao Rodrigo Freire pela sua erudição em lógica e disposição em compartilhar todo esse conhecimento. Agradeço também ao Enéas Nogueira Jr., companheiro do grupo de lógica, rimos juntos todas as vezes que descobrimos como sabemos pouco e riremos ainda mais e por muito tempo. Sou grato também aos meus companheiros de Mestrado, André, Arlane, Diego, Dylene, Gustavo e Silvana. Agradeço aos meus amigos da graduação Enéas, Marcel, Marina e Paulinho, obrigado por me deixarem fazer parte de suas vidas.

Agradeço à Sociedade Macedônia e aos DreadAxe pois foram meus primeiros amigos nessa vida. Obrigado ao Rafael Rothganger, a maior parte dessa dissertação foi escrita no seu computador. Sou muito grato também às pessoas da Masmorra, do Taj e dos Mariachis.

Agradeço aos leitores que passarão seu tempo lendo até o final esses agradecimentos e aos que lerão até o final dessa dissertação, a estes meu obrigado especial.

Resumo

Por uma lógica S entendemos um par $\langle \mathcal{L}, \vdash_S \rangle$ onde $\mathcal{L}$ é um conjunto de conectivos e $\vdash_S$ é o símbolo para a relação de consequência de S. Por matriz semântica $\mathcal{M}$ entendemos um par $\langle \mathbf{A}, D \rangle$, onde $\mathbf{A}$ é uma estrutura algébrica e D é um conjunto de valores designados. Neste trabalho caracterizamos a relação de consequência semântica em $\mathcal{M}$ ($\models_{\mathcal{M}}$) como um polinômio na álgebra $\mathbf{A}$. Por exemplo, dada uma consequência do cálculo proposicional clássico do tipo,

$$A, A \to B \models B,$$

diremos que ela é válida se, e somente se, existirem x, y e z, tais que

$$(a+1) \cdot y + ((a \to b) + 1) \cdot x + b \cdot z = 1.$$

Onde $a, b, c, x, y, z \in \mathbf{BR}$, um anel booleano.

Por meio desse trabalho queremos estudar a existência desses multiplicadores em diversas lógicas, tanto em lógicas clássicas, como a lógica de primeira ordem e as lógicas modais normais, quanto em lógicas não clássicas, como as multivaloradas e a intuicionista.

Palavras Chave: Lógica clássica. Lógica multivalorada, Invariantes algébricos, Anéis booleanos, Álgebra cilindrica, Álgebra boolena com operadores, Semântica matricial.

Abstract

By a logic S we understand a pair $\langle \mathcal{L}, \vdash_S \rangle$ where $\mathcal{L}$ is a set of connectives and $\vdash_S$ is a symbol for the consequence relation of S. By semantic matrix $\mathcal{M}$ we understand a pair $\langle \mathbf{A}, D \rangle$, where $\mathbf{A}$ is a algebraic structure and D is a set of designated values. In this work we caracterize the consequence relation on $\mathcal{M}$ ($\models_{\mathcal{M}}$) as a polynomial over the algebra $\mathbf{A}$. For example, given a consequence on the proposicional classical logic like,

$$A, A \to B \models B,$$

we say it's valid if and only if there are x, y and z, such that

$$(a+1) \cdot y + ((a \to b) + 1) \cdot x + b \cdot z = 1.$$

Where $a, b, c, x, y, z \in \mathbf{BR}$, a boolen ring.

With this work we wish to study the existence of theses multipliers in a diverse number of logics, such as classical logics, like first order logic and normal modal logics, as much as the non-classical logics, like the many-valued logics and intuicionistic logic.

Keywords: Classical logic, Many-valued logic, Algebraic Inariants, Boolean ring, Cilindric algebra, Boolena algebra with operators, Matrix Semantics.

Sumário

1 Introdução **3**
- 1.1 Motivação . . . 3
- 1.2 Objetivos . . . 4
- 1.3 Organização deste trabalho . . . 5

2 Preliminares **7**
- 2.1 Lógica . . . 7
- 2.2 Álgebra Universal . . . 13
- 2.3 Extensões . . . 16
- 2.4 Da lógica para a álgebra . . . 17
- 2.5 Polinômios . . . 19
- 2.6 Corpos Finitos . . . 21
- 2.7 Lógica e anéis de polinômios . . . 21

3 Multiplicadores algébricos de validade clássica **23**

4 Multiplicadores algébricos, outras lógicas **27**
- 4.1 Lógica de 1.ª Ordem . . . 29
- 4.2 Lógicas Modais . . . 30
- 4.3 Lógicas Multivaloradas . . . 31

5 Considerações Finais **39**
- 5.1 Os objetivos foram alcançados? . . . 39
- 5.2 O que ficou em aberto? . . . 39
- 5.3 Trabalhos futuros . . . 40

Capítulo 1

Introdução

O leitor não familiarizado com um campo de estudos como a lógica matemática pode achar que existem poucos tópicos a serem abordados nesse assunto (como exemplo posso citar meus familiares que acreditam que eu passo a maior parte do meu tempo resolvendo revistas de passatempo). Contrariando tal expectativa neste capítulo vamos introduzir algumas definições e termos para que fique claro ao leitor nossa motivação e nossos objetivos neste trabalho.

1.1 Motivação

Vamos definir o cálculo proposicional clássico $\mathcal{C}$ de forma matricial e por ele esclarecer nossos interesses. Considere o seguinte conjunto $\mathcal{A} = \{0, 1\}$ e as operações $\mathcal{F} = \{\cdot, +, \rightarrow\}$, dadas por:

$\cdot$	0	1
0	0	0
1	0	1

$+$	0	1
0	0	1
1	1	0

$\rightarrow$	0	1
0	1	1
1	0	1

Se X é um conjunto de variáveis, uma fórmula em $\mathcal{C}$ é obtida da seguinte forma:

i. se $A \in X$, então A é uma fórmula;

ii. se A e B são fórmulas, então $A \cdot B$, $A + B$ e $A \rightarrow B$ são fórmulas;

iii. nada mais é fórmula.

O conjunto de fórmulas é denotado por Fm. Se A e B são fórmulas as seguintes expressões são fórmulas: $A + A$, $A + 1$, $A \rightarrow (B \rightarrow A)$ e 0. Seja τ uma função tal que $\tau : Fm \rightarrow \mathcal{A}$, com as seguintes restrições:

i. $\tau(0) = 0$;
ii. $\tau(1) = 1$;
iii. $\tau(A + B) = \tau(A) + \tau(B)$;
iv. $\tau(A \cdot B) = \tau(A) \cdot \tau(B)$;
v. $\tau(A \rightarrow B) = \tau(A) \rightarrow \tau(B)$;

dizemos que τ é uma *valuação* e denotamos $\tau(A)$ por A^τ.

Se Δ e Γ são dois conjuntos de fórmulas dizemos que Δ é consequência de Γ (notação: $\Gamma \models \Delta$) se para toda fórmula $A \in \Gamma$, $A^\tau = 1$, então existe $B \in \Delta$ tal que $B^\tau = 1$. Se Γ for vazio e $\Delta = \{A\}$ denotamos $\models A$ e dizemos que A é um *teorema.*

Caracterizaremos essa relação de consequência lógica como um polinômio, por exemplo, dado uma consequência do cálculo proposicional clássico do tipo

$$A \rightarrow B, A \models B,$$

provaremos que essa consequência vale se e somente se existirem x, y e z tais que

$$((a \rightarrow b) + 1)x + (a + 1)y + bz = 1.$$

Onde $x, y, z, a, b, c \in \{0, 1\}$.

Este trabalho tem como motivação investigar essa definição alternativa da relação $\models$.

Cronologicamente os multiplicadores algébricos do cálculo clássico foram os primeiros cuja existência foram demonstradas, esse resultado é de autoria do meu orientador (Finger [6]). Nosso trabalho foi estudar esse teorema e estendê-lo. Daí a necessidade de uma linguagem unificada onde pudéssemos tratar lógicas modais e lógicas multivaloradas em um mesmo texto. A versão do resultado clássico está em sua forma original, entretanto com a unificação da linguagem compactamos as demonstrações e ganhamos expressividade.

1.2 Objetivos

Nosso primeiro objetivo neste trabalho será o seguinte teorema:

Teorema 1.1. *Se $A = (A_i)_{i \leq n}$ e $B = (B_i)_{i \leq m}$, fórmulas do cálculo clássico $\mathcal{C}$, onde $n, m \in \mathbb{N}$, então*

$A \models B$ se, e somente se, para cada valoração τ existem $x = (x_i)_{i \leq n}$ e $y = (y_i)_{i \leq m}$ tais que $(a_1 + 1) \cdot x_1 + \ldots + (a_n + 1) \cdot x_n + b_1 \cdot y_1 + \ldots + b_m \cdot y_m = 1$.

Após demonstrarmos esse resultado vamos procurar uma estrutura algébrica que satisfaça esse teorema. A partir desse ponto produziremos alguns exemplos de lógicas diferentes da proposicional clássica que admitam multiplicadores.

Queremos investigar as lógicas tradicionais como a lógica de primeira ordem e as lógicas modais, encontraremos multiplicadores algébricos também nessas lógicas.

Outra abordagem envolverá as lógicas multivaloradas, queremos encontrar algum meio de caracterizar a relação de consequência nessas lógicas através de polinômios. Nesse processo encontraremos alguns polinômios distintos do inicialmente definido.

1.3 Organização deste trabalho

Como pano de fundo para essa exposição provamos alguns resultados sobre a ligação entre consequência semântica da lógica e polinômios na linguagem.

O primeiro capítulo (Preliminares) apresenta a teoria que utilizamos pelo resto do texto, com as principais definições retiradas de [9], [2], [13] e [10] construímos a linguagem unificada que empregamos pelo trabalho.

No segundo capítulo (Multiplicadores algébricos de validade clássica) demonstramos resultados de nossa autoria, mostramos a existência de multiplicadores para a lógica clássica assim como damos alguns exemplos de como eles não são únicos.

No capítulo três (Multiplicadores algébricos, outras lógicas) provamos a existência de multiplicadores em algumas lógicas relevantes, introduzimos um objeto algébrico que tenhas as propriedades necessárias para a existência de multiplicadores.

Capítulo 2

Preliminares

2.1 Lógica

Há quem diga que exista apenas uma única lógica e há quem diga que existam várias. Independente do ponto de vista, qualquer que seja a lógica em questão, ela possui algumas propriedades. Aqui daremos o nome de lógica pra uma grande quantidade de objetos que compartilham algumas características. As definições e notações referentes ao cálculo clássico seguem as encontradas em [2], aquelas relativas à lógica de primeira ordem seguem as definições de [5] enquanto que alguns comentários foram retirados de [12].

Lógica Proposicional

Lógica estuda o conceito de consequências. Dado um conjunto qualquer $\mathcal{P}$ de *proposições atômicas* queremos saber quais consequências podem ser obtidas a partir dele. Em um primeiro momento encontramos formas de compor duas ou mais proposições, por meio de conectivos. Com eles podemos obter novas expressões a partir de antigas, por exemplo, se A e B forem proposições podemos criar novas expressões do tipo "Se A, então B" ($A \rightarrow B$), "não A" ($\neg A$), "ou A ou B, não ambos" ($A+B$) ou ainda "A é necessário" ($\diamond A$). A lista de conectivos pertinentes é tão extensa que escrevê-la por completo é impraticável. Chamaremos de *alfabeto proposicional* qualquer conjunto $\mathcal{L}$ de conectivos. Quando as proposições são combinadas a partir dos conectivos, as novas expressões obtidas recebem o nome de *fórmulas de* $\mathcal{L}$ ($\mathcal{L}$-fórmulas) e formalmente as construímos em três passos:

i. Se $A \in \mathcal{P}$, então A é uma fórmula;

ii. para cada $f_n \in \mathcal{L}$, conectivo n-ário, se $A_1, \ldots, A_n \in \mathcal{P}$, então $f_n(A_1, \ldots, A_n)$ é fórmula;

iii. Nenhuma outra concatenação de símbolos é fórmula.

Denotamos o conjunto de todas as $\mathcal{L}$-fórmulas por $Fm_{\mathcal{L}}$ ($\mathcal{L}$ é omitido da notação quando for clara a partir do contexto).

Duas observações sobre essa construção. A sentença *ii* abrange os conectivos unários $(\neg A, \diamond A, \ldots)$, os conectivos binários $(A \rightarrow B, A + B, \ldots)$, quaisquer outros conectivos n-ários e inclusive conectivos 0-ários. Por fim, a sentença *iii* nos previne de aceitar patologias do tipo "$\rightarrow AB\diamond$" como fórmulas.

Fixe uma fórmula A do tipo $A_1 \rightarrow A_2$; pela definição de fórmula que demos podemos a partir de A construir uma nova fórmula da seguinte maneira: considere a fórmula $(A_3 + A_4)$ e em A substitua A_2 por $(A_3 + A_4)$, obtendo A' da forma $A_1 \rightarrow (A_3 + A_4)$.

A função que leva A em A' é uma *substituição*, sua notação é definida por:

i. Se A é atômica, $A[A \leftarrow B] = B$;

ii. Se A e atômica e $A \neq B$, $C[A \leftarrow B] = C$;

iii. Se $f \in \mathcal{L}$ e $A_1, \ldots, A_n$ são fórmulas, então $f(A_1, \ldots, A_n)[A \leftarrow B] = f(A_1[A \leftarrow B], \ldots, A_n[A \leftarrow B])$.

A seguinte substituição $(A_1 \rightarrow A_2)[A_2 \leftarrow (A_3 + A_4)] = A_1 \rightarrow (A_3 + A_4)$ foi utilizada em nosso exemplo, geralmente nos referimos a função que leva A em $A[B \leftarrow C]$ por σ e muitas vezes denotamos $A[B \leftarrow C]$ por $\sigma(A)$.

Nosso próximo passo será inferir novas fórmulas a partir de outras anteriormente estabelecidas. Suponha que afirmamos as fórmulas "Se A, então B"e "A". Gostaríamos de afirmar também B, queremos uma forma de expressar em nossa lógica.

Por *inferência* sobre $\mathcal{L}$ queremos dizer um par $\langle \Gamma, A \rangle$, onde Γ é um conjunto finito de fórmulas e A é uma única fórmula. Em notação nosso exemplo seria $\langle \{A \rightarrow B, A\}, B \rangle$. Dizemos que uma fórmula B é *derivada diretamente* de um conjunto Δ de fórmulas pela regra $\langle \Gamma, A \rangle$ se existe uma substituição σ tal que $\sigma(A) = B$ e $\sigma(\Gamma) \subset \Delta$ $(\sigma(\Gamma) = \{\sigma(A) : A \in \Gamma\})$. Em nosso exemplo utilizamos a substituição $\sigma(A) = A_1 + A_2$ e $\sigma(B) = A_3$.

A seguir iremos definir um sistema dedutivo axiomático. Fixe um conjunto qualquer Ax de fórmulas, vamos chamar os elementos de Ax de *axiomas*. Um *sistema dedutivo axiomático* S (sobre $\mathcal{L}$) é definido por um (possivelmente infinito) conjunto de regras de inferência e axiomas, consistindo do par S $= \langle \mathcal{L}, \vdash_S \rangle$, onde $\vdash_S$ é a relação entre conjunto de fórmulas e fórmulas individuais definido como segue: $\Delta \vdash A$ se, e somente, se existe uma sequência de fórmulas $A_1, \ldots, A_n$ com $A_n = A$, onde cada A_i é da seguinte forma:

i. $A_i \in \Delta$, ou;

ii. A_i é alguma substituição de algum axioma, ou;

iii. A_i é derivada diretamente de $\{A_j : j \in J\}$ para algum $J \subset \{1, \ldots, i-1\}$ por alguma regra de inferência.

A sequência $A_1, \ldots, A_n$ é chamada de *dedução.*

Se $\Delta \vdash A$ com Δ vazio, dizemos que A é *teorema* de S. Claramente cada sistema S está ligado a um conjunto de axiomas e regras de inferência. Informalmente nos referimos a sistemas dedutivos como *sistemas lógicos* ou simplesmente *lógica.* A relação $\vdash_S$ é chamada de *relação de consequência* de S. Dizemos que $\Delta_1 \vdash_S \Delta_2$ se $\Delta_1 \vdash_S A$ para algum $A \in \Delta_2$. Tradicionalmente nos referimos a S como um *sistema de Hilbert.*

Esse é um bom momento para um exemplo (Apresentação retirada de [8]).

Exemplo 2.1. *Lógica proposicional clássica* (C)

Nosso alfabeto proposicional é $\mathcal{L} = \{\neg, \vee, \wedge, \rightarrow, \top, \bot\}$.

As seguintes fórmulas serão nossos axiomas:

(lpc_1) $A \rightarrow (B \rightarrow A)$

(lpc_2) $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

(lpc_3) $(C \rightarrow A) \rightarrow ((C \rightarrow B) \rightarrow (C \rightarrow (A \wedge B)))$

(lpc_4) $(A \wedge B) \rightarrow A$

(lpc_5) $(A \wedge B) \rightarrow B$

(lpc_6) $A \rightarrow (A \vee B)$

(lpc_7) $B \rightarrow (A \vee B)$

(lpc_8) $(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow ((A \vee B) \rightarrow C)$

(lpc_9) $(A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A)$

(lpc_{10}) $A \rightarrow (\neg A \rightarrow B)$

(lpc_{11}) $\neg\neg A \rightarrow A$

E nossa regra de inferência será o *Modus ponens*:

(MP) $\langle \{A, A \rightarrow B\}, B \rangle$

A constante $\top$ é abreviação para $A \vee \neg A$.

A constante $\bot$ é abreviação para $A \wedge \neg A$.

Por último, como ilustração das definições, vamos mostrar que $A \rightarrow A$ é um teorema de C:

$\vdash_C A \rightarrow A$,

para tal, vamos construir uma dedução.

A_1. $(A \to (((A \to A) \to A) \to A)) \to ((A \to ((A \to A) \to A)) \to (A \to A)$

A_2. $A \to (((A \to A) \to A) \to A)$

A_3. $(A \to ((A \to A) \to A)) \to (A \to A)$

A_4. $A \to ((A \to A) \to A)$

A_5. $A \to A$

Onde, por (lpc_2), $A_1 = (A \to (B \to C)) \to ((A \to B) \to (A \to C))[B \leftarrow (A \to A)][C \leftarrow A]$.

Por (lpc_1), $A_2 = A \to (B \to A)[B \leftarrow (A \to A)]$.

Com **(MP)** $\langle\{A_1, A_2\}, A_3\rangle$.

Por (lpc_1), $A_4 = A \to (B \to A)[B \leftarrow (A \to A)]$

Com **(MP)** $\langle\{A_3, A_4\}, A_5\rangle$.

Existem métodos mais eficientes e menos heurísticos para desempenhar esse serviço, porém pouco contribuiriam para nosso objetivos no texto.

Como segundo exemplo vamos definir as lógicas modais normais. Retiramos este exemplo de [1].

Exemplo 2.2. *Lógica modal normal* (L_M)

Dado um conectivo ∇, unário, dizemos que ∇ é um *conectivo modal* se sempre que $A \vdash B$, temos que $\nabla A \vdash \nabla B$. Entretanto nem todas as lógicas modais são do nosso interesse nesse exemplo.

Fixe o seguinte alfabeto proposicional $\mathcal{L} = \{\neg, \vee, \wedge, \to, \Box, \Diamond\}$

As seguintes fórmulas serão nossos axiomas:

(lm_0) Os axiomas de (lpc_1) até (lpc_{11})

(K) $\Box(A \to B) \to (\Box A \to \Box B)$

$(Dual)$ $\Diamond A \leftrightarrow \neg\Box\neg A$

(MP) $\langle\{A, A \to B\}, B\rangle$

(Gen.) $\langle\{A\}, \Box A\rangle$

Chamamos esse sistema de lógica **K**, e toda lógica que satisfaça os axiomas (lm_0), (K) e $(Dual)$, com as regras de inferência **(MP)** e **(Gen.)** é chamada de lógica modal normal.

Tradicionalmente consideramos outras lógicas. Considere os seguintes axiomas:

(4) $\Diamond\Diamond A \to \Diamond A$

(T) $\Box A \to A$

(B) $A \to \Box\Diamond A$

Algumas das lógicas modais normais são **T**, **S4**, **B**, e **S5** dadas pela lógica **K** mais o axioma **(T)**, **K** mais os axiomas **(T)** e **(4)**, **K** mais o axioma **(B)** e **K** mais os axiomas **(T)**, **(4)** e **(B)**, respectivamente.

Lógica de Primeira Ordem

Definimos a *lógica de primeira ordem* (LPO) nessa seção de forma a nos referir a ela em nossas demostrações futuras.

Nosso alfabeto de primeira ordem será denotado por $\mathcal{L}_1$. Precisamos de um conjunto para nos referirmos aos objetos do domínio do discurso, denotamos por $\mathbf{X} = \{x_i\}_{i \in \mathbb{N}}$ tal conjunto e chamaremos seus elementos de *variáveis*. Por $\mathcal{C}$, $\mathcal{F}$ e $\mathcal{R}$ denotamos os nomes das *constantes*, *funções* e *relações*, respectivamente. Denotamos por $\mathcal{F}_n$ e $\mathcal{R}_n$ as funções e relações n-árias. Entenda por termo uma sequência de símbolos do tipo:

i. Tanto constantes quanto variáveis são termos;

ii. $f_k(t_1, \ldots, f_k)$, onde $f_k \in \mathcal{F}_k$, t_i ou é uma constante.

Denote por $Term_{\mathcal{L}_1}$ o conjunto de termos de $\mathcal{L}_1$.

Uma *fórmula atômica* é da forma $R_n(t_1, \ldots, t_n)$.

Para caracterizar a lógica de primeira ordem precisamos introduzir um quantificador. Quando tratamos dos objetos em questão queremos expressar uma noção de quantidade, o símbolo $\forall x A$ diz algo como "para todo x A". a partir dele definimos $\exists = \neg\forall x \neg A$ que pode ser entendido como "existe x tal que A". Ambos os conectivos são tradicionalmente chamados de *quantificadores*.

Uma fórmula em $\mathcal{L}_1$ é construída como segue:

i. Uma fórmula atômica é uma fórmula;

ii. se A e B são fórmulas, então também são fórmulas $\neg A$, $A \to B$ e $\forall x A$;

iii. nenhuma outra sequência de símbolos é fórmula.

Denote por $Fm_{\mathcal{L}_1}$ o conjunto de fórmulas de $\mathcal{L}_1$.

Falta-nos algumas noções sobre as variáveis para que possamos continuar.

Quando quantificamos sobre uma variável x (por exemplo, $\forall x(x = x)$) ela se torna *limitada* a esse quantificador, enquanto que se não houver quantificadores sobre x (como em A da forma $\exists y(y = x)$) dizemos que x é *livre em* A.

Considere a fórmula A da forma $x = x$. Denote por $A|_{x=y}$ a operação de substituir todas as ocorrências de x em A por y resultando em $y = y$. Note que nesse primeiro exemplo obtivemos uma fórmula equivalente à inicial, entretanto considere B como $\exists x \neg(x = y)$ e aplique a substituição $B|_{x=y}$ obtendo a fórmula $\exists y \neg(y = y)$ que é muito diferente da anterior. Esse tipo de substituição deve ser evitada, por isso faremos uma restrição a essa operação. Seja x uma variável e t um termo, definimos *t é substituível por x em A* como segue:

i. Para A atômica t é substituível por x em A;

ii. t é substituível por x em $\neg A$ se e somente se t é substituível por x em A, t é substituível por x em $A \rightarrow B$ se e somente se t é substituível por x em A e em B;

iii. t é substituível por x em $\forall y A$ se e somente se:

a. ou x não ocorre livre em $\forall y A$;

b. ou y não ocorre em t e t é substituível por x em A.

Dado as definições acima podemos estabelecer a lógica de primeira ordem.

Exemplo 2.3. A seguinte apresentação foi retirada de [5]. Lógica de primeira ordem (L_1). Nosso alfabeto será composto por $\mathcal{L}_1 = \{\neg, \vee, \wedge, \rightarrow, \forall\}$. As seguintes fórmulas serão nossos axiomas:

(lpo_0) Os axiomas de (lpc_1) até (lpc_{11})

(lpo_1) $\forall x A \rightarrow A|_{t=x}$, onde t é substituível por x em A

(lpo_2) $\forall x(A \rightarrow B) \rightarrow (\forall x A \rightarrow \forall x B)$

(lpo_3) $A \rightarrow \forall x A$, onde x não ocorre livre em A

(MP) $\langle \{A, A \rightarrow B\}, B \rangle$

Se a linguagem incluir o símbolo para igual ($=$) acrescentamos os seguintes axiomas, para cada $R \in \mathcal{R}$ e cada $F \in \mathcal{F}$

(lpo_4) $x = x$

(lpo_5) $x = y \rightarrow (A \rightarrow A')$, onde A é uma fórmula atômica e A' é obtida de A substituindo todos, algum ou nenhum x por y.

Quando nos referimos a uma lógica queremos arbitrar valores às suas fórmulas, dizendo assim se elas são verdadeiras ou falsas, ou quem sabe ainda um terceiro valor. No cálculo clássico tome uma fórmula A e suponha que ela seja verdadeira, queremos que sua negação $\neg A$ seja falsa e ainda que $\neg\neg A$ seja verdadeira. Os símbolos de verdade e falsidade têm um comportamento algébrico e para extrair todas essa informações precisamos de estruturas algébricas pertinentes a cada sistema lógico. Na próxima seção trataremos de diversos objetos algébricos com essa motivação.

2.2 Álgebra Universal

A seguir definimos alguns objetos algébricos, ferramentas de extrema importância em nosso estudo. As definições desta seção foram retiradas de [2] e alguns exemplos de [10].

Um *alfabeto* de álgebras é um conjunto $\mathfrak{F}$ de *símbolos funcionais* tal que um inteiro não negativo n é associado a cada $f \in \mathfrak{F}$. Esse número é chamado de *aridade* de f. O subconjunto de símbolos funcionais n-ários de $\mathfrak{F}$ é denotado por $\mathfrak{F}_n$. Uma *álgebra* $\mathbf{A}$ de *tipo* $\mathfrak{F}$ é um par ordenado $\langle \mathcal{A}, \mathcal{F} \rangle$, onde $\mathcal{A}$ é um conjunto não vazio e $\mathcal{F}$ é uma família de operações em $\mathcal{A}$ indexada pelo alfabeto $\mathfrak{F}$ tal que correspondendo a cada símbolo funcional n-ário f há uma operação n-ária $f^{\mathbf{A}}$ em $\mathcal{A}$. O conjunto $\mathcal{A}$ é chamado de *universo* de $\mathbf{A}$, e as $f^{\mathbf{A}}$'s são chamadas de *operações fundamentais* de $\mathbf{A}$.

A abstração própria dessas definições ficará mais clara com os próximos exemplos:

Exemplo 2.4. Um *grupo* é uma tripla $\langle G, +, 0 \rangle$, onde $\mathfrak{F}_2 = \{+\}$ e $\mathfrak{F}_0 = \{0\}$ tais que as seguintes igualdades são verificadas para qualquer a, b, c:

(g_1) $(a+b)+c = a+(b+c)$;

(g_2) $0+a = a+0 = a$;

(g_3) Existe $-a \in G$, tal que $a+(-a) = (-a)+a = 0$.

(Usualmente escrevemos $a - a$ para $a + (-a)$)

O grupo é chamado de grupo comutativo se além disso satisfaz:

(g_4) $a+b = b+a$.

Um *anel* é uma quadrupla $\langle R, +, \cdot, 0 \rangle$, onde $\mathfrak{F}_2 = \{+, \cdot\}$ e $\mathfrak{F}_0 = \{0\}$ tais que valem as seguintes igualdades:

$(a_0)\langle R, +, 0 \rangle$ é um grupo comutativo (Satisfaz (g_1), (g_2), (g_3), (g_4));

(a_1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(a_2) $(a \cdot (b+c) = a \cdot b + a \cdot c)$ e $((a+b) \cdot c = a \cdot c + b \cdot c)$.

O anel é chamado de anel comutativo se além disso satisfaz:

(a_3) $a \cdot b = b \cdot a$.

O anel é chamado de anel com unidade se:

(a_4) Existe $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a$.

(Usualmente abreviamos $a \cdot b$ por ab)

Um *corpo* é uma quíntupla $\langle K, +, \cdot, 0, 1 \rangle$, onde $\mathfrak{F}_2 = \{+, \cdot\}$ e $\mathfrak{F}_0 = \{0, 1\}$, tais que valem os seguintes axiomas:

$(k_0)\langle K, +, \cdot, 0 \rangle$ é um anel comutativo com unidade;

(k_1) $1 \neq 0$;

(k_2) Se $a \neq 0$, então existe $a^{-1} \in K$ tal que $a \cdot a^{-1} = 1$.

Exemplo 2.5. Uma *álgebra booleana* é dada por $\mathbf{B} = \langle B, \vee, \wedge, \neg, 1, 0\rangle$, com $\mathfrak{F}_2 = \{\vee, \wedge\}$, $\mathfrak{F}_1 = \{\neg\}$ e $\mathfrak{F}_0 = \{0, 1\}$, satisfazendo as seguintes igualdades:

(b_1) $a \vee b = b \vee a$
(b_2) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
(b_3) $a \vee 0 = a$
(b_4) $a \vee \neg a = 1$
(b_5) $a \wedge b = b \wedge a$
(b_6) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
(b_7) $a \wedge 1 = a$
(b_8) $a \wedge \neg a = 0$

Um *anel booleano* é dado por $\mathbf{BR} = \langle B, +, \cdot, 0, 1\rangle$, com
(ab_0) $\langle B, +, \cdot, 0, 1\rangle$ é um anel com unidade
(ab_1) $a \cdot a = a$

Um exemplo de álgebra booleana é a álgebra de conjuntos $\langle \wp(X), \cup, \cap, \setminus, \emptyset\rangle$, onde X é um conjunto qualquer, não vazio, e $\wp(X)$ representa o conjunto de todos os subconjuntos de X, $\cup, \cap, \setminus$ são a união, a intersecção e o complementar em relação a X, respectivamente, e $\emptyset$ é o conjunto vazio.

Sempre podemos obter um anel booleano a partir de uma álgebra booleana, para tal defina a soma e multiplicação do anel booleano como segue:
i. $a + b = (a \cdot \neg b) \vee (\neg a \cdot b)$;
ii. $a \wedge b = a \cdot b$

A definição de álgebra cilíndrica abaixo foi retirada de [9].

Exemplo 2.6. Uma *álgebra cilíndrica* é uma sequência
$\mathbf{AC} = \langle A, \vee, \cdot, -, 0, 1, \exists x_\kappa, x_\kappa \approx x_\lambda\rangle_{\kappa,\lambda \in \mathbb{N}}$, com $\mathfrak{F}_2 = \{\vee, \cdot\}$, $\mathfrak{F}_1 = \{-, , \exists x_\kappa\}_{\kappa \in \mathbb{N}}$ e $\mathfrak{F}_0 = \{1, 0, x_\kappa \approx x_\lambda\}_{\kappa,\lambda \in \mathbb{N}}$ e:

(C_0) a estrutura $\langle A, \vee, \cdot, -, 0, 1\rangle$ é uma álgebra booleana;
(C_1) $\exists x_\kappa 0 = 0$;
(C_2) $a \leq \exists x_\kappa a (i.e., (a \vee \exists x_\kappa a) = \exists x_\kappa a)$;
(C_3) $\exists x_\kappa (a \cdot \exists x_\kappa b) = \exists x_\kappa a \cdot \exists x_\kappa b$;
(C_4) $\exists x_\kappa \exists x_\lambda a = \exists x_\lambda \exists x_\kappa a$;
(C_5) $(x_\kappa \approx x_\kappa) = 1$;
(C_6) se $\kappa \neq \lambda, \mu$, então $(x_\lambda \approx x_\mu) = \exists x_\kappa((x_\lambda \approx x_\kappa) \cdot (x_\kappa \approx x_\mu))$;
(C_7) se $\kappa \neq \lambda, \mu$, então $\exists x_\kappa((x_\kappa \approx x_\lambda) \cdot a) \cdot \exists x_\kappa((x_\kappa \approx x_\lambda) \cdot -a) = 0$.

O seguinte exemplo foi retirado de [1].

Exemplo 2.7. Uma *álgebra booleana com operadores* é da forma **ABO** $= \langle B, \vee, \cdot, \neg, 0, 1, f\rangle$ com $\mathfrak{F}_2 = \{\vee, \cdot\}$, $\mathfrak{F}_1 = \{\neg, f\}$ e $\mathfrak{F}_0 = \{0, 1\}$, onde:

(abo_0) $\langle B, \vee, \cdot, \neg, 0, 1\rangle$ é uma álgebra booleana

(abo_1) $f(a \vee b) = f(a) \vee f(b)$;

(abo_2) $f(0) = 0$

A lógica também estuda o conceito de verdade. Dado um conjunto de proposições gostaríamos de saber quais são verdadeiras e quais são falsas. Como fazer isso exatamente veremos na próxima seção, entretanto podemos definir lógicas partindo dessa propriedade. Por exemplo, definindo quais fórmulas serão as verdadeiras e quais regras de inferências preservarão a validade. Podemos até mesmo propor outros modelos com valores verdade além do verdadeiro e falso. Os detalhes serão vistos com a linguagem abaixo.

Uma *Matriz* é um par $\mathscr{A} = \langle \mathbf{A}, D\rangle$, onde $\mathbf{A}$ é uma Álgebra e $D \subsetneq \mathcal{A}$. Os elementos de D são chamados de *valores designados*. Se X é um conjunto não vazio e disjunto de $\mathcal{A}$, denotamos por $Term_{\mathbf{A}}$ o menor conjunto tal que

i. $X \cup \mathfrak{F}_0 \subset Term_{\mathbf{A}}$ e

ii. se $a_1, \ldots, a_n \in Term_{\mathbf{A}}$ e $f^{\mathbf{A}} \in F_n$, então $f^{\mathbf{A}}(a_1, \ldots, a_n) \in Term_{\mathbf{A}}$.

$Term_{\mathbf{A}}$ é o conjunto de *termos* de **A**, e X é o conjunto de *variáveis* (omitimos o índice da álgebra quando não houver perigo de confusão). Seja v uma função tal que $\tau : Term_{\mathbf{A}} \to \mathcal{A}$, onde $\tau(f(a_1, \ldots, a_n)) = f(\tau(a_1), \ldots, \tau(a_n)$, para cada $f_n \in \mathfrak{F}_n$ e $a_1, \ldots, a_n \in Term_{\mathbf{A}}$. Dizemos que τ é uma *interpretação*. Se o conjunto de proposições atômicas $\mathcal{P}$ e variáveis X tiverem a mesma cardinalidade podemos definir uma tradução $t : Fm_{\mathcal{L}} \to Term_{\mathbf{A}}$, tomando $t(A_i) = x_i$, se $\mathcal{L}$ e **A** tiverem o mesmo alfabeto. Também damos o nome de interpretação para a composição $\tau \circ t$, denotamos $\tau(A)$ por A^τ.

Seja $\mathcal{M}$ uma classe de matrizes, se Γ e Δ são conjuntos de termos em **A**, dizemos que Δ é *consequência semântica* de Γ em $\mathcal{M}$ (simbolicamente, $\Gamma \vDash_{\mathcal{M}} \Delta$) se para todo $\langle \mathbf{A}, D\rangle \in \mathcal{M}$ e toda interpretação τ de $\mathcal{A}$, temos que $A^\tau \in D$, para todo $A \in \Gamma$, então $B^\tau \in D$ para algum $B \in \Delta$. Quando $\mathcal{M}$ estiver claro vamos omiti-lo da notação, transformando os símbolos em $\Gamma \vDash \Delta$.

Uma matriz $\mathscr{A}$ é chamada de *matriz modelo* de S (S um sistema dedutivo) se $\Gamma \vdash_S A$ implica que $\Gamma \vDash_{\mathscr{A}} A$ para todo $\Gamma \cup \{A\} \subset Fm_{\mathbf{A}}$. Um subconjunto D de **A** é chamado se *S-filtro*, ou simplesmente *filtro* quando S estiver claro a partir do contexto, se a matriz $\langle \mathbf{A}, D\rangle$ é uma matriz modelo de S. Daí D é um S-filtro se, e somente, se D contém todas as interpretações dos axiomas de S e é fechado sobre cada regra de inferência $\langle \Gamma, A\rangle$ (no sentido que $\Gamma \vDash_{\mathscr{A}} A$).

Definição 2.8. Seja S $= <\mathcal{L}, \vdash_S>$ um sistema dedutivo e $\mathcal{M}$ uma classe de matrizes. $\mathcal{M}$ é chamada de *semântica matricial* de S se, para todo $\Gamma \cup \{A\} \subset Fm$, $\Gamma \vdash_S A \Leftrightarrow \Gamma \vDash_{\mathcal{M}} A$.

Exemplo 2.9. Vamos definir de forma matricial a lógica proposicional clássica (C). Por convenção chamamos de verdade o valor 1 e de falso o valor 0.

$\mathcal{A} = \{0, 1\}$
$\mathcal{F} = \{\wedge, \neg\}$
$D = \{1\}$

$\wedge$	0	1
0	0	0
1	0	1

	$\neg$
0	1
1	0

Exemplo 2.10. *Lógica trivalorada de Lukasiewicz.* A lógica de três valores de Łukasiewicz pode ser definida da seguinte forma:

$\mathcal{A} = \{0, 1, 2\}$
$\mathcal{F} = \{\neg, \rightarrow\}$
$D = \{2\}$

$\rightarrow$	0	1	2
0	2	2	2
1	1	2	2
2	0	1	2

	$\neg$
0	2
1	1
2	0

Exemplo 2.11. *Lógica Infinita de Łukasiewicz.*

Seja $(\mathbb{R}, +, \cdot, 0, 1)$ o corpo dos números reias, seja $I = [0, 1] \subset \mathbb{R}$, defina a lógica infinita de Łukasiewicz como:

$\mathcal{A} = I \cap \mathbb{Q}$
$\mathcal{F} = \{\neg, \rightarrow\}$
$D = \{1\}$
$\neg A = 1 - A$
$A \rightarrow B = min\{1, 1 - A + B\}$

2.3 Extensões

A definição de extensões que vamos utilizar foi retirada de [12].

Definição 2.12. A lógica $S' = \langle \mathcal{L}', \vdash_{S'} \rangle$ é *extensão conservativa* da lógica $S = \langle \mathcal{L}, \vdash_S \rangle$ se :

i. S' estende S: Se $\vdash_S A$, então $\vdash_{S'} A$;

ii. S' é conservativa sobre S: Se $\vdash_{S'} A$ e $A \in Fm_{\mathcal{L}}$, então $\vdash_S A$.

Nesse caso S é chamada de *fragmento conservativo* de S'.

Teorema 2.13. *Sejam S e S' duas lógicas e sejam $\mathcal{M}$ e $\mathcal{M}'$ suas respectivas matrizes semânticas. Se S' for extensão conservativa de S então:*

i. $\vDash_{\mathcal{M}} \subset \vDash_{\mathcal{M}'}$;

ii. $D = D' \cap \boldsymbol{A}'$, *para todo* $\langle \boldsymbol{A}, D \rangle \in \mathcal{M}$ *e* $\langle \boldsymbol{A}', D' \rangle \in \mathcal{M}'$

Demonstração. *i.* é simples verificação. *ii.* fixada uma matriz $\langle \mathbf{A}, D \rangle \in \mathcal{M}$, seja um elemento $d \in D$, assim $\vDash_{\mathcal{M}} d$ e como S' é extensão de S, temos de $\vDash_{\mathcal{M}'} d$, daí $d \in D'$ para toda matriz $\langle \mathbf{A}', D' \rangle \in \mathcal{M}'$ □

Definição 2.14. Seja $\mathbf{A} = (\mathscr{A}, \mathscr{F})$, uma álgebra. Recursivamente definimos:

$$i.\quad \begin{array}{ll} \pi_i & : \mathscr{A}^n \to \mathscr{A} \text{ é operação primitiva de } \mathscr{A} \\ \pi_i : & \quad (a_i)_{i \leq n} \mapsto a_i \end{array}$$

ii. se $(x_1, \ldots, x_n)$ são operações primitivas em $\mathscr{A}$, então $f(x_1, \ldots, x_n)$ é operação primitiva de $\mathscr{A}$, para cada $f \in \mathscr{F}_n$, $n \in \mathbb{N}$.

*iii.*Nenhuma outra operação é operação primitiva.

Quando uma função for primitiva em $\mathscr{A}$, diremos que ela é obtida em função dos operadores em $\mathscr{F}$.

Teorema 2.15. *Seja S um sistema dedutivo, e $\mathcal{M}$ sua matriz semântica. Para cada $\langle \boldsymbol{A}, D \rangle \in \mathcal{M}$, se $\mathscr{G}$ for um conjunto de operadores primitivos de $\mathscr{A}$, a nova classe de matrizes obtida por $\langle \boldsymbol{A}', D \rangle$, onde $\boldsymbol{A}' = \langle \mathscr{A}, \mathscr{G} \rangle$ dá origem à uma lógica S' que é fragmento conservativo de S.*

2.4 Da lógica para a álgebra

Nesta seção vamos unir a lógica à álgebra.

Uma observação sobre a notação. Usualmente iremos denotar as fórmulas lógicas por letras latinas maiúsculas $(A, B, C, \ldots)$ e termos algébricos por latinas minúsculas $(a, b, c, \ldots)$. Quando traduzirmos uma fórmula de um sistema lógico para sua respectiva matriz utilizaremos as letras minúsculas correspondentes, por exemplo, $A \to B$ traduzido se tornará $a \to b$ em vez de $A^\tau \to B^\tau$.

A seguinte definição foi retirada de [1].

Definição 2.16. Uma equação $a \approx b$ é *verdade* ou *válida* em uma álgebra $\mathbf{A}$ (notação: $\models_{\mathbf{A}} a \approx b$), se para toda valuação τ, $\tau(a) = \tau(b)$. Um conjunto Γ de equações é *verdade* ou *válido* em uma álgebra $\mathbf{A}$ se para cada $a \approx b \in \Gamma$ tivermos que $\models_{\mathbf{A}} a \approx b$. Dizemos que $a \approx b \in \Gamma$ é verdade em uma classe de álgebras $\mathfrak{A}$ se $\models_{\mathbf{A}} a \approx b$ ($\models_{\mathbf{A}} \Gamma$) para toda álgebra $\mathbf{A} \in \mathfrak{A}$. Denotamos por $\Gamma \models_{\mathfrak{A}} a \approx b$ sempre que se Γ for verdade em toda álgebra $\mathbf{A} \in \mathfrak{A}$, então $\models_{\mathbf{A}} a \approx b$.

Dado um conjunto Γ de fórmulas denote por $\Gamma^{\approx} = \{a \approx \top : A \in \Gamma\}$. O próximo teorema foi retirado de [1].

Teorema 2.17. *Denote por $\mathcal{BR}$ a classe dos anéis booleanos.*

$$\Gamma \vdash_{\mathcal{C}} A \textit{ se, e somente se, } \Gamma^{\approx} \models_{\mathcal{BR}} a \approx \top$$

O seguinte teorema foi retirado de [11].

Teorema 2.18. *Denote por $\mathcal{AC}$ a classe das álgebras cilíndricas.*

$$\Gamma \vdash_{L_1} A \textit{ se, e somente se, } \Gamma^{\approx} \models_{\mathcal{AC}} a \approx \top$$

Para um conjunto Σ de fórmulas de uma lógica modal normal, seja $\bigvee_{\Sigma}$ a classe das álgebras booleanas com operadores tal que o conjunto $\Sigma^{\approx}$ é válido.

O próximo teorema foi retirado de [1].

Teorema 2.19. *Seja Σ um conjunto de fórmulas de uma lógica modal normal. Se $\boldsymbol{K}\Sigma$ for a lógica modal normal axiomatizada por Σ, então*

$$\Gamma \vdash_{\boldsymbol{K}\Sigma} A \textit{ se, e somente se, } \Gamma^{\approx} \models_{\bigvee_{\Sigma}} a \approx \top$$

Exemplo 2.20. Neste exemplo vamos ilustrar o teorema 2.19. Nas hipóteses do teorema se Σ for vazio $\bigvee_{\Sigma}$ é a classe das álgebras booleanas com operadores como no exemplo 2.7.

Por outro lado se $\Sigma = \{\Box A \to A\}$ (axioma **T**), $\bigvee_{\Sigma}$ seria a seguinte estrutura algébrica:

ABO $= \langle B, \vee, \cdot, \neg, 0, 1, \Diamond \rangle$ com $\mathfrak{F}_2 = \{\vee, \cdot\}$, $\mathfrak{F}_1 = \{\neg, \Diamond\}$ e $\mathfrak{F}_0 = \{0, 1\}$, onde:

(abo_0) $\langle B, \vee, \cdot, \neg, 0, 1 \rangle$ é uma álgebra booleana

(abo_1) $\Diamond(a \vee b) = \Diamond(a) \vee \Diamond(b)$;

(abo_2) $\Diamond(0) = 0$

(t) $a \cdot \Box a = \Box a$

Se $\Sigma = \{\Box A \to A, \Diamond\Diamond A \to \Diamond A, A \to \Box\Diamond A\}$ (axiomas **T**, **4** e **B**), referente a lógica **S5**, as relações algébricas seriam:

(t) $a \cdot \Box a = \Box a$

(4) $(\Diamond\Diamond a) \cdot (\Diamond a) = \Diamond\Diamond a$

(b) $a \cdot \Diamond\Box a = a$

Se $\Sigma = \{\Box A \to A, \Diamond\Diamond A \to \Diamond A, A \to \Box\Diamond A\}$ (axiomas **T**, **4** e **B**), referente à lógica **S5**, além de (abo_0), (abo_3) e (abo_2) as relações algébricas seriam:

(t) $a \cdot \Box a = \Box a$

(4) $(\Diamond\Diamond a) \cdot (\Diamond a) = \Diamond\Diamond a$

(b) $a \cdot \Diamond\Box a = a$

2.5 Polinômios

A seguir definimos a noção de polinômios para qualquer álgebra.

Definição 2.21. Dada uma álgebra $\mathbf{A}$ definimos o conjunto $\mathbf{A}[\mathrm{X}]$ dos polinômios nas variáveis $X = \{x_1, \ldots, x_n\}$ como o menor conjunto tal que:

i. $X \cup A \subset \mathbf{A}[X]$;

ii. se $a_1, \ldots, a_n \in \mathbf{A}[X]$ e $f^{\mathbf{A}} \in F_n$, então $f^{\mathbf{A}}(a_1, \ldots, a_n) \in \mathbf{A}[X]$.

Exemplo 2.22. Em uma álgebra booleana podemos ter como exemplos de polinômios, $(x_1 \to a_1) \cdot x_2$ ou $((\neg a_1) \cdot x_1) \to (x_1 \cdot x_1)$. Em um anel booleano seria algo como $((\neg a_1) \cdot x_1) + (a_2 \cdot b)$.

A noção de polinômios mais recorrente na teoria de corpos também será útil, por isso enunciamos o seguinte teorema. Os teoremas e definições a seguir foram extraídos de [10].

Teorema 2.23. *Seja R um anel e denote por $R[x_1, \ldots, x_n]$ o conjunto de todas as funções $f : \mathbb{N}^n \to R$ tal que $f(u) \neq 0$ para no máximo uma quantidade finita de elementos $u \in \mathbb{N}^n$.*

i. *$R[x_1, \ldots, x_n]$ é um anel com adição e multiplicação definidas por:*

$$(f+g)(u) = f(u) + g(u) \quad e \quad (fg)(u) = \sum_{\substack{v+w=u \\ v,w \in \mathbb{N}^n}} f(v)g(w)$$

ii. Se $\boldsymbol{R}$ *é comutativo (respectivamente anel com unidade),* $R[x_1, \ldots, x_n]$ *também o é.*

iii. Seja $\boldsymbol{R}$ *um anel com unidade e* $\varepsilon_i = (0, \ldots, 1, \ldots, 0) \in \mathbb{N}^n$*. Para cada* $i \leq n$ *seja* $x_i \in R[x_1, \ldots, x_n]$ *tal que* $x_i(\varepsilon_i) = 1$ *e* $x_i(u) = 0$ *se* $u \neq \varepsilon_i$*. Então para cada polinômio não nulo* $f \in R[x_1, \ldots, x_n]$ *existem únicos elementos não nulos* $(k_{11}, \ldots, k_{1n}), \ldots, (k_{m1}, \ldots, k_{mn})$ *de* $\mathbb{N}^n$ *e únicos elementos* $a_0, \ldots, a_m$ *de* R*, tais que*

$f = a_0 x_1^0 \ldots x_n^0 + a_1 x_1^{k_{11}} \ldots x_n^{k_{1n}} + \ldots + a_m x_1^{k_{m1}} \ldots x_n^{k_{mn}}$.

Chamamos de grau de f *o número* $\partial(f) = max\{k_{j1} + \ldots + k_{jn} : k_{ji}$ *é dado como acima*$\}$

□

Seja K um corpo e $f \in K[x]$ um polinômio de grau positivo. f é dito redutível sobre K se f pode ser escrito como produto de fatores lineares em $K[x]$, isto é, $f = a_0(x - a_1) \ldots (x - a_n)$, onde $a_i \in K$. Caso contrário f é dito irredutível.

Definição 2.24. K é um subcorpo de F se $K \subset F$ e K for um corpo. Também chamamos F de *extensão de corpo* de K. Se F é uma extensão de corpo de K e $X \subset F$, então o *subcorpo gerado* por $K \cup X$ será a intersecção de todos os subcorpos de F, contendo $K \cup X$ e será denotado por $K(X)$.

Teorema 2.25. *O subcorpo* $K(X)$ *consiste de todos os elementos da forma*

$$\frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} = f(a_1, \ldots, a_n) \cdot g(a_1, \ldots, a_n)^{-1}$$

onde $n > 0$, $\quad f, g \in K[x_1, \ldots, x_n] \quad$ *e* $\quad a_1, \ldots, a_n \in X$.

Definição 2.26. Seja K um corpo e $f \in K[x]$ um polinômio de grau positivo, $a \in K$ é dito *raiz* de f se $f(a) = 0$.

Definição 2.27. Seja K um corpo e $f \in K[x]$ um polinômio de grau positivo. Uma extensão de corpo F é dita um *corpo de decomposição* sobre K do polinômio f se f é redutível em $F[X]$ e $F = K(a_1, \ldots, a_n)$ onde $a_1, \ldots, a_n$ são as raízes de f em F.

Definição 2.28. Seja $(K, +, \cdot, 1, 0)$ um corpo, denotamos por K^* o grupo $(K \setminus \{0\}, \cdot, 1)$ e o chamamos de *grupo multiplicativo*.

2.6 Corpos Finitos

Definição 2.29. Fixe $n \in \mathbb{N}$ e $z \in \mathbb{Z}$, denote por:

$$\overline{z}_n = \{x \in \mathbb{Z} : \text{o resto da divisão de } x - z \text{ por } n \text{ é } 0 \ \}.$$

Como exemplo, $\overline{1}_2 = \{\ldots, -1, 1, 3, 5, 7, \ldots\}$, $\overline{0}_2 = \{\ldots, -2, 0, 2, 4, \ldots\}$, $\overline{4}_3 = \{\ldots, -2, 1, 4, 7, 10, \ldots\}$. Perceba ainda que $\overline{1}_3 = \overline{4}_3 = \overline{7}_3 = \overline{10}_3$ Denote por $\mathbb{Z}_n = \{\overline{0}_n, \overline{1}_n, \ldots, \overline{n-1}_n\}$, por mera verificação o leitor pode perceber que $\overline{n}_n = \overline{0}_n$, $\overline{n+1}_n = \overline{1}_n$ etc. Denote por $+$ e $\cdot$ a soma e a multiplicação usual de $\mathbb{Z}$, seja $a, b \in \mathbb{Z}$, defina as seguintes operações sobre $\mathbb{Z}_n$:

i. $\overline{a}_n +_n \overline{b}_n = \overline{(a+b)}_n$

ii. $\overline{a}_n \cdot_n \overline{b}_n = \overline{(a \cdot b)}_n$

Teorema 2.30. *Fixe $n \in \mathbb{N} \setminus \{0\}, n \geq 2$ e $z \in \mathbb{Z}$:*

i. $\langle \mathbb{Z}_n, +, \cdot, \overline{0}, \overline{1} \rangle$ é um anel;

ii. Se n for primo $\langle \mathbb{Z}_n, +, \cdot, \overline{0}, \overline{1} \rangle$ é um corpo.

Teorema 2.31. *Seja p um primo e k um inteiro positivo. Existe um corpo finito com p^k elementos. Além disso, qualquer corpo finito tem p^k elementos (para algum p e algum k) e é isomorfo ao corpo de decomposição de $x^{p^k} - x$ sobre $\mathbb{Z}_p$.*

Denotaremos tal corpo por $\mathbb{F}_{p^k}$

Demonstração. Vide [10]

□

2.7 Lógica e anéis de polinômios

Vamos utilizar as definições estabelecidas até aqui e enunciar um resultado que nos permitirá traduzir as lógicas multivaloradas para a linguagem polinomial. Esse resultado é devido à Carnielli e sua demostração pode ser visto em [4].

Teorema 2.32. *[Representações de operações finitas em corpos finitos]*

Seja A um conjunto qualquer de cardinalidade $|A| = k$, $k \in \mathbb{N} \setminus \{0\}$ e $f : A^m \mapsto A$ uma operação m-ária sobre A. Sejam p, um primo, e n, um natural, tais que $p^n \geq k$. Então f pode ser representado como um polinômio em $\mathbb{Z}_{p^k}[x_1, \ldots, x_n]$.

Exemplo 2.33. Vamos utilizar o teorema em algumas lógicas para que tudo isso fique mais claro para o leitor.

Lógica clássica Com $k = 2$, $p = 2$ e $n = 1$, cada um dos operadores lógicos $\{\neg, \wedge, \vee, \rightarrow\}$ se transformam nos seguintes polinômios em $\mathbb{Z}_2$(exemplo retirado de [4]):
$D = \{1\}$

C		$\mathbb{Z}_2[x,y]$
$\neg x$	$\mapsto$	$x + 1$
$x \wedge y$	$\mapsto$	$x \cdot y$
$x \vee y$	$\mapsto$	$x \cdot y + x + y$
$x \rightarrow y$	$\mapsto$	$x \cdot y + x + 1$

Lógica trivalorada de Łukasiewicz Com $k = 3$, $p = 3$ e $n = 1$, a lógica de Łukasiewicz apresenta os seguintes polinômios (exemplo retirado de [3]):
$D = \{2\}$

$Ł_3$		$\mathbb{Z}_3[x,y]$
$\neg x$	$\mapsto$	$2x + 2$
$x \rightarrow y$	$\mapsto$	$2x \cdot (y+1) \cdot (x \cdot y + y + 1) + 2$

Capítulo 3

Multiplicadores algébricos de validade clássica

Neste capítulo definiremos a noção de multiplicadores de validade.

Definição 3.1. Seja **BR** um anel booleano e seja também $a = (a_i)_{i \leq n}$ e $b = (b_i)_{i \leq m}$, $n, m \in \mathbb{N}$ termos de **BR**. Considere o seguinte polinômio de $n + m$ variáveis:

$P_{ab}(x, y) = \neg a_1^\tau \cdot x_1 + \ldots + \neg a_n^\tau \cdot x_n + b_1^\tau \cdot y_1 + \ldots + b_m^\tau \cdot y_m$.

P_{ab} é chamado de *polinômio especial* de **BR**. Dizemos que x e y são *1-raízes* ou *multiplicadores algébricos* de P_{ab} se $P_{ab}(x, y) \in 1$.

Perceba que poderíamos definir tal polinômio em qualquer álgebra que tenha os conectivos $\neg$, $\cdot$ e $+$.

Nos próximos resultados iremos caracterizar a relação $\vDash$ pela existência de multiplicadores algébricos. O teorema 3.5 foi demonstrado em [6]. Diremos que um conjunto Γ é *inconsistênte* se para toda valoração τ existe $A \in \Gamma$ tal que $A^\tau = 0$. Note que isso é o mesmo que $\Gamma \vDash 0$.

Lema 3.2. *Seja $\Gamma = \{A_1, \ldots, A_n\} \subset Fm_{\mathcal{L}}$, se Γ é inconsistênte em C ($\Gamma \vDash_C 0$), então existem $x_1, \ldots, x_n \in$ **BR** tais que*

$$\sum_{i=1}^{n} x_i \cdot (a_i + 1) = 1$$

Demonstração. Por indução em n. Para o caso base, considere $n = 1$, então A_1 é uma fórmula inconsistente. Como resultado $a_1 = 0$, basta tomar $x_1 = 1$. Assim $(a_1) \cdot x_1 = (0 + 1) \cdot 1 = 1$

Suponha que o conjunto $\{A_1, \ldots, A_{n+1}\}$ com $n+1$ elementos seja inconsistente; então o conjunto $\{A_1, \ldots, A_n \wedge A_{n+1}\}$ com n elementos é claramente inconsistente, e nós podemos aplicar a hipótese de indução, então existem $x_1, \ldots, x_n$ tais que:

$$\sum_{i=1}^{n-1} x_i \cdot (a_i + 1) + x_n \cdot (a_n \cdot a_{(n+1)} + 1) = 1$$

Para resolver essa equação é suficiente obter x'_n e x'_{n+1} tais que

$$x'_n \cdot (a_n + 1) + x'_{n+1} \cdot (a_{n+1} + 1) = x_n \cdot (a_n \cdot a_{(n+1)} + 1)$$

Existem muitas possíveis soluções para essa equação. Podemos tomar $x'_n = x_n \cdot a_{n+1}$ e $x'_{n+1} = x_n$; ou $x'_n = x_n \cdot (a_n \cdot a_{n+1} + 1)$ e $x'_{n+1} = x_n \cdot a_n$. Em ambos os casos obtemos os multiplicadores para Γ.

□

Exemplo 3.3. Considere o conjunto de fórmulas inconsistênte $\Gamma = \{A, C \rightarrow \neg A, B \rightarrow C, B\}$, é simples de verificar que:

$$1 \cdot (a + 1) + 1 \cdot (ca) + a \cdot (b(c + 1)) + a \cdot (c + 1) \cdot (b + 1) = 1,$$

então uma possível atribuição para os multiplicadores seria $1, 1, a, a(c + 1)$.

Lema 3.4. *Seja $\Gamma = \{A_1, \ldots, A_n\} \subset Fm_{\mathcal{L}}$, tais que $\sum_{i=1}^{n} x_i \cdot (a_i + 1) = 1$, onde $x_1, \ldots, x_n \in \boldsymbol{BR}$. Então Γ é inconsistênte em C ($\Gamma \vDash_C 0$).*

Demonstração. Provamos por indução em n. Para o cado base $n = 1$ temos $x_1 \cdot (a_1 + 1) = 1$, que é válida se e somente se $x_1 = a_1 + 1$. Daí $a_1 = 0$ e Γ é inconsistente.

Considere $\sum_{i=1}^{n} x_i \cdot (a_i + 1) = 1$. Multiplicando ambos os lados por $a_1 \cdot a_2$ os primeiros dois termos são cancelados e depois de algum reagrupamento obtemos

$$\sum_{i=3}^{n} (a_1 \cdot a_2 \cdot x_i) \cdot (a_i + 1) = a_n \cdot a_2.$$

Adicionando $a_1 \cdot a_2 + 1$ em ambos os lados temos

$$\sum_{i=3}^{n}(a_1 \cdot a_2 \cdot x_i) \cdot (a_i + 1) + (a_1 \cdot a_2 + 1) = 1.$$

O lado esquerdo a igualdade é uma soma de $n-1$ termos, onde o multiplicador do último termo é 1. Pela hipótese de indução, obtemos que o conjunto $\{A_1 \wedge A_2, \ldots, A_n\}$ é inconsistênte, logo Γ é inconsistênte.

$\square$

Teorema 3.5. *Seja* $\Gamma = \{A_1, \ldots, A_n, B_1, \ldots, B_m\} \in Fm_{\mathcal{L}}$. $A_1, \ldots, A_n, \vDash_{\mathcal{C}} B_1, \ldots, B_m$ *se, e somente se, existirem* $X = (X_1, \ldots, X_n), Y = (Y_1, \ldots, Y_m) \in Fm_{\mathcal{L}}$ *tais que* $P_{AB}(x, y) = 1$

Demonstração. Se $A_1, \ldots, A_n, \vDash_{\mathcal{C}} B_1, \ldots, B_m$ então o conjunto $\{A_1, \ldots, A_n, \neg B_1, \ldots, \neg B_m\}$ é inconsistênte. Assim aplicando lema 3.2, obtemos os multiplicadores.

Por outro lado, se os multiplicadores existem, pelo lema 3.4, $\{A_1, \ldots, A_n, \neg B_1, \ldots, \neg B_m\}$ é inconsitênte, então $A_1, \ldots, A_n, \vDash_{\mathcal{C}} B_1$. $\square$

Exemplo 3.6. Na lógica proposicional clássica fixe uma fórmula qualquer $A \in Fm_{\mathcal{L}}$, sabemos que $A \vDash A$ então vamos encontrar os multiplicadores dessa fórmula. Considere $x = 1$ e $y = 1$, daí:

$$(a+1) \cdot x + a \cdot y = a + 1 + a = 1$$

Por outro lado se considerarmos $x = a + 1$ e $y = a$ teríamos:

$$(a+1) \cdot x + a \cdot y = (a+1) \cdot (a+1) + a \cdot a = a + 1 + a = 1$$

Note que $a + a = 2 \cdot a = 0$ e que $a \cdot a = a$ pois fazemos as operações em $\mathbb{Z}_2$.

Ou seja, os multiplicadores x e y não são únicos.

Com o Teorema 3.5 fica demonstrada a possibilidade de caracterizar a relação semântica através de polinômios, com isso o trabalho de encontrar teoremas na lógica é transferido para o de encontrar raízes de polinômios. O que faremos no resto do texto será exibir outra lógicas onde possamos fazer o mesmo tipo de caracterização.

Capítulo 4

Multiplicadores algébricos, outras lógicas

Seja S uma lógica, dado um conectivo c diremos $c \in \mathcal{L}$ se c for uma abreviação de conectivos em $\mathcal{L}$. Suponha que existam conectivos unários e binários em $\mathcal{L}$, vamos denotá-los por $-, \odot$ e $\oplus$. Seja $\mathcal{M}$ uma semântica matricial para S. Tome $\langle \mathbf{A}, D \rangle \in \mathcal{M}$ e considere $A_1, \ldots, A_n, B_1, \ldots, B_m \in Fm_{\mathcal{L}}$, para n, m inteiros positivos e τ uma valoração em $\mathbf{A}$. Seja $P_{AB}(X, Y) = ((-a_1) \odot x_1) \oplus \ldots \oplus ((-a_n) \odot x_n) \oplus (b_1 \odot y_1) \oplus \ldots \oplus (b_m \odot y_m)$ um polinômio em $\mathbf{A}[x, y]$ e o chamamos de *polinômio especial* de S para as fórmulas $A_1, \ldots, A_n$, $B_1, \ldots, B_m$. Note que $X = (X_1, \ldots, X_n)$ e $Y = (Y_1, \ldots, Y_m)$. Se existirem $X, Y \in Fm_{\mathcal{L}}$ tais que $P_{AB}(x, y) \in D$ para toda τ e para toda matriz $\langle \mathbf{A}, D \rangle \in \mathcal{M}$, então X e Y serão considerados *multiplicadores algébricos* das fórmulas em questão.

Pergunta Quais propriedades S deve satisfazer para que um conjunto de fórmulas $\{A_1, \ldots, A_n, B_1, \ldots, B_m\}$ admita multiplicadores algébricos se, e somente se, $A_1, \ldots, A_n \vdash_S B_1, \ldots, B_m$? Quais lógicas que conhecemos satisfazem tais propriedades?

Definição 4.1. Diremos que uma lógica S *admite* multiplicadores algébricos se o seguinte resultado é valido:

Qualquer conjunto de fórmulas $\{A_1, \ldots, A_n, B_1, \ldots, B_m\}$ admite multiplicadores algébricos, se e somente se, $A_1, \ldots, A_n \vDash_S B_1, \ldots, B_m$.

Nos capítulos anteriores tratamos as álgebras e as matrizes como objetos separados, sem que as operações presentes na álgebra mencionassem o conjunto de valores designados e vice e versa. No parágrafo seguinte vamos definir abstratamente uma classe de matrizes a partir das propriedades que gostaríamos que ela possuísse. Logo a seguir mostramos que existem alguns representantes dessa classe.

Definição 4.2. *Matriz de multiplicadores*

Seja $\mathcal{A} = \langle \mathbf{A}, D \rangle$ uma matriz. $\mathcal{A}$ será uma *matriz de multiplicadores* se existe $\mathfrak{F}_1 = \{\neg\}$, $\mathfrak{F}_2 = \{+, \cdot\}$, $1 \in D$ e $0 \in \mathbf{A} \setminus D$ satisfazendo as seguintes propriedades (onde d, d_1, d_2 e d_3 são elementos quaisquer de D, f, f_1, f_2 e f_3 são elementos quaisquer de $\mathbf{A} \setminus D$ e $a, b, c \in \mathbf{A}$):

(am_1) $\neg d = f$
(am_2) $\neg f = d$
(am_3) $a \cdot f_1 = f_2$
(am_4) $f_1 \cdot a = f_2$
(am_5) $d_1 \cdot d_2 = d_3$
(am_6) $a + (b + c) = (a + b) + c$
(am_7) $f_1 + f_2 = f_3$
(am_8) $d_1 + d_2 = f$
(am_9) $d_1 + f = d_2$
(am_{10}) $a + b = b + a$

Note que por (am_3) e (am_4) não temos que $f_1 \cdot a = a \cdot f_1$, o que os axiomas nos dizem são que, por exemplo, por (am_3) temos que $f_1 \cdot a \in D$ e que por (am_1) $\neg d \notin D$.

Se redefinirmos o polinômio especial de **BR** de forma apenas a depender dos conectivos, independente da álgebra, podemos escrever o seguinte resultado:

Teorema 4.3. *Multiplicadores de validade lógica* Dada uma matriz $\mathcal{P} = \langle AM, +, \cdot, \neg, 0, 1, F, D \rangle$, onde $\langle AM, +, \cdot, \neg, D \rangle$ é uma matriz de multiplicadores e F é um conjunto qualquer de operadores, $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_m)$ onde $a, b \in AM$, então

$a \vDash_{\mathcal{P}} b$ se, e somente se, para cada valoração τ existem $x = (x_i)_{i \leq n} \in AM$ e $y = (y_i)_{i \leq m} \in AM$ tais que $P_{ab}(x, y) \in D$.

Demonstração. Para simplificar a notação tratamos f e d como algum elemento de $\mathbf{A} \setminus D$ e D, respectivamente e denotamos a_i^τ por a_i.

($\Rightarrow$)Primeiro suponha que $a_1, \ldots, a_n \vDash b_1, \ldots, b_m$. Fixado uma valoração τ, se $a_k^\tau \in D$ para todo $k \leq n$, então

$\neg(a_1)\cdot x_1+\ldots+\neg(a_n)\cdot x_n+b_1\cdot y_1+\ldots+b_m\cdot y_m=f+b_1\cdot y_1+\ldots+b_m\cdot y_m$, como $a_1,\ldots,a_n\vDash b_1,\ldots,b_n$ existe $r\leq m$ tal que $b_r\in D$, assim tomando $y_r=d$, $y_s=f$ se $r\neq s$ e $x_k=f$ para todo $k\leq n$, temos que $\neg(a_1)\cdot x_1+\cdots+\neg(a_n)\cdot x_n+b_1\cdot y_1+\cdots+b_m\cdot y_m=b_r\cdot d\in D$, logo $b_r\in D$. Se $a_i\in \mathbf{A}\setminus D$ para algum $i\leq n$, basta tomar $x_i=d$, $x_j=f$ se $i\neq j$, e $y_k=f$ para todo $k\leq m$.

($\Leftarrow$)Agora, suponha que existem $x,y\in AM^{n+m}$ tais que $\neg(a_1)\cdot x_1+\cdots+\neg(a_n)\cdot x_n+b_1^{\cdot}y_1+\cdots+b_m\cdot y_m\in D$ para toda valoração τ. Se $a_i^\tau\notin D$, para algum $i\leq n$, o resultado é imediato; se $a_i\in D$, para todo $i\leq n$ temos que $b_1\cdot y_1+\cdots+b_m\cdot y_m\in D$, daí existe $r\leq m$, tal que $b_r\cdot y_r\in D$, isto é, $b_r\in D$, portanto $a_1,\ldots,a_n\vDash b_1,\ldots,b_n$ □

Perceba que o Teorema 3.5 é um caso particular desse último resultado com $\mathcal{A}=\{0,1\}$ e $D=\{1\}$.

Exemplo 4.4. Vamos a um exemplo de álgebra de multiplicadores que dá origem a uma lógica triavalorada.

Considere $AM=\{0,\epsilon,1\}$, $D=\{1\}$ e $\mathscr{F}=\{+,\cdot,\neg\}$.

$+$	0	ϵ	1
0	0	ϵ	1
ϵ	ϵ	ϵ	1
1	1	1	ϵ

$\cdot$	0	ϵ	1
0	0	0	0
ϵ	0	ϵ	ϵ
1	0	0	1

	$\neg$
0	1
ϵ	1
1	0

Note que $\epsilon\vDash\epsilon$, pois se $x=1$ e $y=0$, o seu polinômio especial seria $\neg\epsilon\cdot x+\epsilon\cdot y=1$. Por outro lado $1\nvDash\epsilon$, pois para qualquer y o polinômio especial $(\neg 1\cdot x+\epsilon\cdot y=1)$ não tem solução.

4.1 Lógica de 1.ª Ordem

Vamos olhar para a lógica de primeira ordem.

Considere a seguinte matriz $\mathscr{AC}=\langle\mathbf{AC},\{1\}\rangle$, onde **AC** é uma álgebra cilíndrica, com isso podemos enunciar o seguinte teorema (lembrando que $\mathcal{L}_1$ é o alfabeto da lógica de primeira ordem):

Teorema 4.5. *Seja* $\Gamma=\{A_1,\ldots,A_n,B_1,\ldots,B_m\}\in Fm_{\mathcal{L}_1}$. $A_1,\ldots,A_n,\vDash_{AC}B_1,\ldots,B_m$ *se, e somente se, existirem* $X=(X_1,\ldots,X_n),Y=(Y_1,\ldots,Y_m)\in Fm_{\mathcal{L}_1}$ *tais que* $P_{AB}(x,y)=1$

Demonstração. Basta lembrar que uma álgebra cilíndrica é uma extensão de um anel booleano, daí pelo Teorema 4.3 temos o resultado.

$\square$

Exemplo 4.6. Vamos provar $\models \forall x(R(x_1) \to R(x_1))$, seu polinômio especial é $P(y) = (-\exists x_1 - (R(x_1) \to R(x_1)) \cdot y$, fazendo $y = \forall x(R(x_1) \to R(x_1))$, temos $P(y) = (-\exists x_1 - (R(x_1) \to R(x_1)) \cdot y = (-\exists x_1 - (R(x_1) \to R(x_1)) = -\exists x_1 - \top = -\exists x_1 \bot = -\bot = \top$.

4.2 Lógicas Modais

A demonstração da versão do resultado para lógicas modais é similar à primeira ordem.

Teorema 4.7. *Seja $\mathcal{L}_M$ uma lógica modal normal.*

$\Gamma = \{A_1, \ldots, A_n, B_1, \ldots, B_m\} \in Fm_{\mathcal{L}_M}$. $A_1, \ldots, A_n \models_{\mathcal{L}_M} B_1, \ldots, B_m$ *se, e somente se, existirem* $X = (X_1, \ldots, X_n), Y = (Y_1, \ldots, Y_m) \in Fm_{\mathcal{L}_M}$ *tais que* $P_{AB}(x, y) = 1$.

Exemplo 4.8. Considere a lógica modal normal **K**, de $\square(A \cdot B) \models \square A$ obtemos o polinômio $P(x, y) = -\square(a \cdot b) \cdot x + \square a \cdot y)$, daí $P(\top, \square b) = -\square(a \cdot b) \cdot \top + \square a \square b = -\square(a \cdot b) + \square a \square b = \top$. A última igualdade vale pois $\neg a = a + 1$ e $\square(a \cdot b) = (\square a) \cdot (\square b)$.

Exemplo 4.9. Considere a lógica modal normal **T**, e lembre que a seguinte igualdade vale: $a \cdot \square a = \square a$.

Considere a fórmula $\square A \to \Diamond A$, vamos provar que $\models_{\mathbf{T}} \square A \to \Diamond A$.

Tomando $Y = 1$, note que $(\square a \to \Diamond a) \cdot Y = \square a \cdot \Diamond a + \square a + 1 = \square a \cdot (\square(a + 1) + 1) + \square a + 1 = \square a \cdot \square(a+1) + \square a + \square a + 1 = \square(a \cdot (a+1)) + 1 = \square 0 + 1 = 1$, pois em **T** verifica-se que $\square 0 = 0 \cdot \square 0 = 0$.

por outro lado, podemos provar o seguinte:

$\square A \models_{\mathbf{T}} \Diamond A$, onde seu polinômio é $((\square a + 1) \cdot x + (\square(a + 1) + 1) \cdot y)$, com multiplicadores $x = 1$ e $y = \square a$.

Ainda podemos percorrer um outro caminho. Podemos provar:

$\square A \to A, A \to \Diamond A \models \square A \to \Diamond A$, onde seu polinômio é
$(\square a \cdot a + \square a)x + (a \cdot (\square(a + 1) + 1) + a)y + (\square a \cdot (\square(a + 1) + 1) + \square a + 1)z$, com os multiplicadores $x = \square(a + 1)$, $y = 1$ e $z = a \cdot (\square 0 + \square(a + 1)) + 1$

Como em **T**, $\vdash \square A \to A$ e $\models A \to \Diamond A$, temos outra prova de $\square A \to \Diamond A$.

4.3 Lógicas Multivaloradas

O teorema abaixo é enunciado para que possamos estudar a existência de multiplicadores algébricos em extensões de lógicas multivaloradas finitas. Por hora é importante para o leitor perceber o encavalamento de símbolos nesse texto. Não confunda o '+' presente nas álgebras de multiplicadores com o '+' presente nos corpos e álgebras booleanas. Esse cuidado deve ser tomado para os conectivos '$\neg$' e '$\cdot$'. Os corpos admitem sua própria versão do Teorema 4.3.

Teorema 4.10. *Seja K um corpo $(a_i)_{i\leq n}, (b_j)_{j\leq m} \in K$. Seja $\theta : K \to K$ uma operação unária qualquer sobre K e $D \subsetneq K$ não vazio. São equivalentes as afirmações:*

1. Se para todo $i \in \{1, \ldots, n\}$ $a_i \in D$, então para algum $j \in \{1, \ldots, m\}$ $b_j \in D \iff$ existem $(x_i)_{i\leq n}, (y_j)_{j\leq m} \in K$ tais que $(\theta(a_1)x_1 + \ldots + \theta(a_n)x_n + b_1y_1 + \ldots + b_ny_n) \in D$.

2. $D = K^*$ e $(\theta(a) \notin D \leftrightarrow a \in D)$

Demonstração. 1. $\to$ 2. Vamos supor que a equivalência da propriedade 1 é válida e vamos provar o item 2.

• $D = K^*$

Seja $z \in K^*$ e $d \in D$. Para $x = 0$ e $y = \frac{d}{z}$, temos que $(\theta(d) \cdot x + z \cdot y) = d \in D$. Logo, como $d \in D$ temos também que $z \in D$. Daí $K^* \subset D$, como $D \subsetneq K$ temos que $0 \notin D$. Portanto $D = K^*$.

• $\theta(a) \notin D \to a \in D$

Suponha que $a \notin D$, assim para qualquer x e y, $(\theta(a) \cdot x + a \cdot y) \notin D$, o que é absurdo.

• $a \in D \to \theta(a) \notin D$

Suponha que $\theta(a) \in D$ e para algum $d \in D$ e $b \notin D$ tome $x = \frac{d}{\theta(a)}$ e $y = 0$ e note que $(\theta(a) \cdot x + b \cdot y) = d \in D$. Como $b \notin D$, temos que $a \notin D$.

2. $\to$ 1. Agora supomos as propriedades do item 2 e provamos a equivalência do item 1.

Suponha que se para todo $i \in \{1, \ldots, n\}$ $a_i \in D$, então para algum $j \in \{1, \ldots, m\}$ $b_j \in D$

Vamos provar que existem $(x_i)_{i\leq n}, (y_j)_{j\leq m} \in K$ tais que
$(\theta(a_1)x_1 + \ldots + \theta(a_n)x_n + b_1y_1 + \ldots + b_ny_n) \in D$.

Se $a_i \in D$ para todo $i \leq n$, então $\theta(a_i) \notin D$, isto é, $\theta(a_i) = 0$. Podemos tomar $y_j = 1$ e $y_l = 0$ se $l \neq j$ daí:
$(\theta(a_1)x_1 + \ldots + \theta(a_n)x_n + b_1y_1 + \ldots + b_ny_n) = b_j \in D$

Se $a_i \notin D$ para algum $i \leq n$, então $\theta(a_i) \in D$, e basta tomar $x_i = 1$ e $x_n = 0$ se $n \neq i$ e $y_j = 0$, e assim:

$(\theta(a_1)x_1 + \ldots + \theta(a_i)x_i + \ldots + \theta(a_n)x_n + b_1y_1 + \ldots + b_ny_n) = \theta(a_i) \in D$

Por outro lado suponha que existem $(x_i)_{i\leq n}, (y_j)_{j\leq m} \in F$ tais que $(\theta(a_1)x_1 + \ldots + \theta(a_n)x_n + b_1y_1 + \ldots + b_ny_n) \in D$, daí vamos provar que se para todo $i \in \{1, \ldots, n\}$ $a_i \in D$, então para algum $j \in \{1, \ldots, m\}$ $b_j \in D$.

Se existem $(x_i)_{i\leq n}, (y_j)_{j\leq m} \in K$ tais que $(\theta(a_1)x_1 + \ldots + \theta(a_n)x_n + b_1y_1 + \ldots + b_jy_j) \in D$, e $a_i \in D$ para todo $i \in \{1, \ldots, n\}$, temos que $b_1y_1 + \ldots + b_jy_j \in D$. Por hipótese, $b_1y_1 + \ldots + b_jy_j \neq 0$ logo, para algum l, $b_ly_l \neq 0$ e assim $b_l \in D$.

□

θ nesse teorema tem o papel da negação no caso clássico e mostra quais propriedades ela precisa ter para satisfazer o teorema.

Não sabemos se todo sistema lógico admite multiplicadores algébricos, entretanto muitas dessas lógicas são extensões de outras que admitem tal propriedade ou ainda podemos estender a lógica para que ela esteja contida em um sistema dedutivo que admita multiplicadores.

Primeiramente vamos enunciar um resultado que nos permitirá decidir de forma rápida quando uma lógica multivalorada, de valores finitos pode ser estendida até um novo sistema dedutivo que admita multiplicadores.

Antes de enunciarmos o teorema principal vamos construir lógicas multivaloradas em $\mathbb{Z}_{p^k}$ a partir de qualquer matriz $\mathcal{M}$ com $\mathcal{A}$ finito. Lembre-se leitor, que por $\mathbb{F}_{p^k}$ denotamos o corpo finito de p^k elementos, que nada mais é que o corpo de decomposição de $x^{p^k} - x$ sobre $\mathbb{Z}_p$ (Teorema 2.32).

Definição 4.11. Seja $\mathcal{M}$ uma classe de matrizes finitas (para toda matriz $\langle \mathbf{A}, D\rangle \in \mathcal{M}$, temos que $\mathcal{A}$ é finito finito). Chamaremos de $\mathcal{M}_z$ a nova classe de $\langle \mathbf{A}_z, D_z\rangle$ obtida por $\iota : \mathcal{A} \to \mathbb{F}_{p^k}$, uma função injetora, onde $|\mathcal{A}| \leq p^k$, construída da seguinte forma.

i. $\mathcal{A}_z \doteq \mathbb{F}_{p^k}$;

ii. $D_z \doteq \mathbb{F}_{p^k} \setminus \{\iota(x) : x \notin D\}$;

iii. $f_z(x) \doteq \iota(f(x))$, se $x \in \mathcal{A}$ e $f_z(x) = 0$ se $x \notin Im(\iota)$, $i \in \mathbb{N}$, para toda $f \in \mathcal{F}$;

iv. Fm_z é o conjunto de fórmulas dessa nova lógica.

$Im(\iota)$ é a imagem de ι.

ι é chamada de *renomeação*. Perceba que para cada ι, $\mathcal{L}_z$ é um novo objeto. A rigor deveríamos indicar isso na notação, mas para evitar acúmulo de símbolos vamos deixar isso livre de notação acreditando que não haverá dificuldades para o leitor.

Não há uma notação unificada das diversas lógicas multivaloradas encontradas nos livros e textos sobre o assunto, em nosso contexto queremos unificar os símbolos empregados nessas lógicas denotando todos os valores por números inteiros, por exemplo:

Exemplo 4.12. Considere a seguinte lógica:
$\mathcal{A} = \{\perp, \top\}$
$D = \{\top\}$
$\mathcal{F} = \{\theta, \omega\}$

ω	$\perp$	$\top$
$\perp$	$\perp$	$\perp$
$\top$	$\perp$	$\top$

	θ
$\perp$	$\top$
$\top$	$\perp$

Vamos construir $\langle \mathbf{A}_z, D_z \rangle$ a partir da renomeação $\iota : \mathbf{A} \longrightarrow \mathbb{Z}_2$, onde $\iota(\perp) = 0$ e $\iota(\top) = 1$, por simples verificação percebemos que ι satisfaz os itens *i.* à *iv.* da definição anterior, dando origem ao cálculo clássico, na linguagem anteriormente estabelecida.

Perceba que a partir dessa unificação de linguagem podemos utilizar o teorema 2.32 para qualquer lógica multivalorada, com valores finitos.

Dito isso vamos ao primeiro resultado de nossa seção.

Teorema 4.13 (Dualidade Polinomial Multivalorada). *Seja $\mathcal{M}$ uma classe de matrizes finitas de ordem p^k (para todo $\langle \boldsymbol{A}, D \rangle \in \mathcal{M}, |\mathcal{A}| \leq p^k$, onde p é primo e k inteiro positivo) com a seguinte restrição, para toda $\langle \boldsymbol{A}, D \rangle \in \mathcal{M}$ existe $\top, \perp \in Fm$ tal que para toda valoração τ temos $\tau(\top) \in D$ e $\tau(\perp) \notin D$, existe uma renomeação ι de forma que dado $\Gamma = (A_1, \ldots, A_n) \cup (B_1, \ldots, B_m) \subset Fm$, e $\tau : Fm_z \longrightarrow \mathbb{F}_{p^k}$ uma valoração das fórmulas da linguagem. As seguintes propriedades são equivalentes:*

1.$A_1, \ldots, A_n \vDash_{\mathcal{M}} B_1, \ldots, B_m$ se, e somente se, existem $x_1, \ldots, x_n, y_1, \ldots, y_m \in \mathscr{A}$ tal que $(\neg(a_1) \cdot x_1 + \ldots + \neg(a_n) \cdot x_n + b_1 \cdot y_1 + \ldots + b_m \cdot y_m) \in D$ para toda τ (lembrando que a_i^τ denotamos por a_i).

2. $D_z = \boldsymbol{A}_z \setminus \{0\}_z$ e $f_z(a) \notin D_z \leftrightarrow a \in D_z$, onde $\mathbb{F}_{p^k}$

Demonstração. A renomeação ι que precisamos é obtida com a seguinte restrição: se $\bot \notin D$, então $\iota(\bot) = 0$.

Observando as fórmulas de Fm e as valuações τ basta repetir os passos da demonstração do Teorema 4.10. □

Vamos a alguns exemplos para ajudar o leitor a perceber o que está acontecendo.

Exemplo 4.14. Neste exemplo ilustraremos uma lógica que satisfaz o teorema, mas para perceber isso teremos de aplicar alguma renomeação. Considere a seguinte lógica:

$\mathcal{A} = \{e, \alpha, \beta, \gamma, \delta, \epsilon\}$;
$D = \{\alpha, \beta, \gamma\, \delta, \epsilon\}$;
$\mathcal{F} = \{f\}$.

Denote por ξ^n a n-ésima raiz da unidade ($\xi^n = 1$), daí

$\mathcal{A}_z = \{e, 1, \xi^1, \xi^2, \xi^3, \xi^4\}$;
$D_z = \{1, \xi^1, \xi^2, \xi^3, \xi^4\}$;
$\mathcal{F}_z = \{f_z\}$.

Onde f,f_z e ι são dados por

	f
e	γ
α	e
β	e
γ	e
δ	e
ϵ	e

$\iota(e) = 0$
$\iota(\alpha) = 1$
$\iota(\beta) = \xi^1$
$\iota(\gamma) = \xi^2$
$\iota(\delta) = \xi^3$
$\iota(\epsilon) = \xi^4$

	f_z
0	ξ^3
1	0
ξ^1	0
ξ^2	0
ξ^3	0
ξ^4	0

Exemplo 4.15. Neste exemplo exibiremos uma lógica onde o teorema 4.13 não é válido e ainda encontraremos uma condição suficiente para que, dada uma lógica S, S admite extensão conservativa S' onde o teorema 4.13 é válido.

Vamos verificar que a lógica trivalorada de Lukasiewicz ($Ł_3$), vista no exemplo 2.33, é um exemplo em que o teorema não é válido. Note que o polinômio $\neg d_2 X + d_1 Y$ tem D-raiz por outro lado $d_2 \not\vDash d_1$, onde d_2 e d_1 são constantes para 2 e 1 respectivamente.

Mas ainda assim, não existe uma lógica que a estenda e ainda assim satisfaça o teorema. Para perceber tal resultado considere a classe de matrizes $\mathcal{M}$ e suponha que ela estenda $Ł_3$, tome $\langle \mathbf{A}, D\rangle \in \mathcal{M}$, pelo teorema 2.13 $\{2\} = D \cap \{0, 1, 2\}$, daí $1 \notin D$, hipótese necessária para o teorema 4.13

Podemos enunciar o seguinte resultado cuja demonstração é a simples repetição do argumento do exemplo acima.

Corolário 4.16. *Seja S uma lógica multivalorada tal que se $\mathcal{M}$ é a classe de matrizes semânticas de S e para cada $\langle \mathbf{A}, D\rangle \in \mathcal{M}$, $\mathcal{A}$ é finito, então uma condição necessária para que exista S' com $\{+,\cdot,\neg\} \subset \mathcal{L}'$ extensão conservativa de S tal que o teorema 4.13 seja válido é que $D_z = \mathcal{A}_z \setminus \{0\}$.*

Por outro lado, mesmo que uma lógica não admita extensão conservativa com multiplicadores como no teorema 4.13 podemos obter um fragmento da lógica que admita multiplicadores. Isso é um pouco mais comum e o resultado será construtivo.

Exemplo 4.17. Considere a lógica Ł$_3$, em primeiro lugar neste exemplo iremos construir um fragmento conservativo de Ł$_3$ que admita multiplicadores. Em seguida vamos construir um novo polinômio especial em Ł$_3$ mostrando que a lógica trivalorada de Łukasiewicz admite multiplicadores de validade. Vamos recordar a matriz de Ł$_3$:

$\mathcal{A}_3 = \{0, 1, 2\}$

$\mathcal{F} = \{\neg, \to\}$

$D = \{2\}$

$\to$	0	1	2
0	2	2	2
1	1	2	2
2	0	1	2

	$\neg$
0	2
1	1
2	0

Faça as seguintes abreviações em Ł$_3$:

$-A \doteq A \to 1$

$A \odot B \doteq -(A \to (-B))$

$A \times B \doteq \neg - (A \odot B)$

$A \triangle B \doteq -((\neg A) \odot (\neg B))$

$A \oplus B \doteq ((-A) \times B)\triangle(A \times (-B))$

Daí as matrizes dos operadores $\odot, \oplus$ e $-$ ficam:

$\odot$	0	1	2
0	1	1	1
1	1	1	1
2	1	1	2

$\oplus$	0	1	2
0	1	1	2
1	1	1	2
2	2	2	1

	$-$
0	2
1	2
2	1

Considere S_3 como a seguinte lógica, $\mathbf{A} = \langle \mathcal{A}_3, \mathcal{G} \rangle$:
$\mathcal{A}_3 = \{0, 1, 2\}$
$\mathcal{G} = \{-, +, \cdot\}$
$D = \{2\}$

Pelo Teorema 2.15 S_3 é fragmento conservativo de Ł_3 e perceba que $\langle \mathbf{A}, D \rangle$ satisfaz os axiomas da definição 4.2. Por exemplo, $2 + 2 = 1$ ou $0 \cdot 1 = 1$ e $0 \cdot 2 = 1$. Portanto S_3 admite multiplicadores algébricos.

Além disso a própria Ł_3 admite multiplicadores algébricos, entretanto seu polinômio especial não é tão simples quanto em S_3. Por exemplo, considere o teorema $\vDash_{\text{Ł}_3} A \to A$, seu polinômio especial seria

$((a \to a) \to (y \to 1)) \to 1$

Enquanto que o polinômio de $A \vDash_{\text{Ł}_3} A$ deixamos para o leitor perceber o quanto cresce o polinômio se escrevermos utilizando apenas os conectivos $\neg$ e $\to$.

Podemos utilizar o Teorema 2.32 e reescrever o polinômio em função dos símbolos $+$ e $\cdot$. Vamos aos conectivos anteriormente abreviados:

Lembrando que:
$\neg A \doteq 2A + 2$
$A \to B \doteq 2A \cdot (B + 1) \cdot (A \cdot B + B + 1) + 2$

Temos:
$-A \doteq A^2 + 2A + 2$
$A \odot B \doteq A^2B^2 + 2A^2B + 2AB^2 + AB + 1$
$A \oplus B \doteq A^2B^2 + 2A^2B + 2AB^2 + AB + 2A^2 + 2B^2 + A + B + 1$

E como referência:
$A \times B \doteq A^2B^2 + 2A^2B + 2AB^2 + AB$
$A \triangle B \doteq A^2B^2 + 2A^2 + 2B^2 + 2$

Com essas definições o polinômio de $A \vDash_{\text{Ł}_3} A$, em função dos símbolos $+$ e $\cdot$ é:

$$(2A^2X^2 + A^2X + AX^2 + 2AX + 2X^2 + X + 1)(A^2Y^2 + 2A^2Y + 2AY^2 + AY + 1)$$

com os multiplicadores $X = 2$ e $Y = 2$.

Dado um conjunto de fórmulas $\{A_1, \dots, A_n, B_1, \dots, B_m\}$, $A_1, \dots, A_n \vDash B_1, \dots, B_m$ tem o seguinte polinômio:

$$\prod_{i=1}^{n}(2A_i^2X_i^2 + A_i^2X_i + A_iX_i^2 + 2A_iX_I + 2X_i^2 + X_i + 1) \prod_{j=m}^{m}(B_j^2Y_j^2 + 2B_j^2Y_j + 2B_jY_j^2 + B_jY_j + 1)$$

Definição 4.18. Dizemos que uma classe de matrizes $\mathcal{M}$ *funcionalmente completa* se para cada $\langle \mathbf{A}, D \rangle \in \mathcal{M}$ e para qualquer operação n-ária $g : \mathcal{A}^n \to \mathcal{A}$, g pode ser obtida em função das operações de $\mathcal{F}$

Com essas elucidações podemos enunciar o seguinte teorema:

Teorema 4.19. *Seja S um sistema lógico onde sua matriz semântica é funcionalmente completa, então S admite multiplicadores algébricos.*

Note que a própria Ł$_3$ não é funcionalmente completa.

Provamos nesse capítulo que as lógicas mais tradicionais admitem multiplicadroes algébricos. No exemplo 4.17 ficou claro por que o polinômio especial terá uma forma diferente para cada lógica, enquanto que no exemplo 4.14 percebemos por que devemos abandonar os axiomas de corpo na estrutura de matrizes de multiplicadores e utilizar os axiomas da definição 4.2.

Capítulo 5

Considerações Finais

5.1 Os objetivos foram alcançados?

Como desejado, mostramos a existência de multiplicadores algébricos em algumas lógicas, entre elas a lógica clássica e suas extensões. Definimos as matrizes de multiplicadores, estruturas com menos propriedades que os anéis booleanos e que admitem multiplicadores algébricos.

Curiosamente nossa primeira impressão quando iniciamos esse trabalho foi de que nenhuma outra lógica pudesse admitir multiplicadores, pois estávamos lidando com lógicas subestruturais (intuicionista, linear, etc.), até que as matrizes de multiplicadores permitiram a exibição de alguns exemplos.

O resultado do Carnielli (Teorema 2.32) permitiu estender a noção de polinômios especias nas lógicas multivaloradas finitas e motivou a definição das matrizes de multiplicadores.

5.2 O que ficou em aberto?

Alguns pontos importantes foram pouco explorados nesse trabalho.

O primeiro ponto entre eles são as lógicas subestruturias, que basicamente são obtidas a partir da lógica clássica retirando-se alguma de suas propriedades, por exemplo:

Exemplo 5.1. Considere a lógica *intuicionista* dada pelos axiomas de (lpc_1) até (lpc_{10}), do exemplo 2.1 (Retirado de [8]). Com $\mathbf{I} = \langle \mathcal{I}, \vdash_{\mathbf{I}} \rangle$, onde $\mathcal{I} = \{\neg, \vee, \wedge, \rightarrow, \top, \bot\}$, temos que a fórmula $A \vee \neg A$ não é um teorema de $\mathbf{I}$ ($\nvdash_{\mathbf{I}} A \vee \neg A$), porém temos que $\vdash_{\mathbf{I}} \neg\neg(A \vee \neg A)$.

Vamos mostrar que o polinômio especial da lógica clássica não serve no caso intuicionista.

Considere o seguinte teorema:

$A \vee \neg A \vdash_{\mathbf{I}} A \vee \neg A$,

entretanto note que nem sempre $a \vee \neg a = 1$, já que $A \vee \neg A$ não é teorema. Assim,

$\neg(a \vee \neg a) \wedge x + (a \vee \neg a) \wedge y = 1$

não tem solução.

Um segundo ponto que não abordamos no texto é um sistema de dedução para uma matriz de multiplicadores, gostaríamos de um conjunto de axiomas e regras de inferência que tivessem como matriz semântica uma matriz de multiplicadores, entretanto até o presente ponto podemos utilizar os axiomas da matriz como metateoremas sobre um candidato à lógica.

Por último nos falta exibir uma lógica que não admita multiplicadores. Uma candidata a isso seria uma lógica que não admite matriz semântica, porém fica em aberto a seguinte conjectura:

Conjectura 5.2. *Seja S uma lógica.*

S admite matriz semântica se, e somente se, S admite multiplicadores algébricos.

5.3 Trabalhos futuros

Inicialmente temos alguns projetos, como ampliar o número de exemplos interessantes que admitam multiplicadores. O primeiro passo nesse sentido foi a lógica $Ł_3$.

Queremos também investigar as lógicas subestruturais mais tradicionais, como a lógica linear, a lógica relevante e a intuicionista.

Um problema que queremos resolver é o de provar ou exibir contraexemplo do teorema 5.2, que se for verdade limitaria nosso trabalho e que se fosse refutado abriria a possibilidade de dividir as lógicas entre as que admitem e as que não admitem multiplicadores.

Por último gostaríamos de publicar nossas ideias em algum periódico da área.

Referências Bibliográficas

[1] P. BlackBurn, M. de Rijke e Y. Venema, *Modal Logic*, Cambridge University Press, 2001.

[2] W.J. Blok., D. Pigozzi., *Algebrizable logics*, American mathematical society, Rhode island, Memoirs of the american mathematical society, January 1989, v. 77, Number 396(third of 4 numbers).

[3] W. Carnielli, *Polynomial Ring Calculus for logical inference*, 2005.

[4] W. Carnielli, *Polynomizing: logic Inference in polynomial Format and the Legacy of Boole*, 2006.

[5] H. B. Enderton, *A mathematical introduction to logic*, Academic Press, New york and London, 1972.

[6] M. Finger, *Entailment Multipliers and their Applications to Proof Theory*, draft version, 2007.

[7] D. Gabbay and F. Guenthner, *Handbook of Philosofical Logic Volume III: Alternatives to classical logic*, D.Reidel Publishing Company, 1986.

[8] N. Galatos, P. Jipsen, T. Kowalski e H. Ono, *Resituated Lattices: An algebraic Glimpse at Substructural Logics*, Elsevier, Amsterdan - Boston - Heidelberg - London - New York - Oxford - Paris - San Diego - San Francisco - Singapore - Sydney - Tokyo, 2007.

[9] L. Henkin, J. D. Monk, A. Tarski, *Cylindric Algebras - part I*, North-Holland Publishing Company Amsterdam-London, 1971.

[10] T.W. Hungerford, *Algebra*, University of Washinton, holt Rinehart and Winston INC. 1973.

[11] J. D. Monk, *Mathematical logic*, Springer-Verlag New York Heldelberg Berlin, 1976.

[12] G. Restall, *An introduction to substructural logics*, Routledge, London and New York

[13] H.P. Sankappanarvar, *A course in Universal Algebra*, Springer-Verlag New York Heldelberg Berlin, 1981.