Mariana Matulovic da Silva

Demonstrações na Algibeira: Polinômios como um Método Universal de Prova

Campinas
2013

Universidade Estadual de Campinas
Instituto de Filosofia e Ciências Humanas - IFCH

Mariana Matulovic da Silva

Demonstrações na Algibeira: Polinômios como um Método Universal de Prova

Tese de doutorado apresentada ao Instituto de Filosofia e Ciências Humanas como parte dos requisitos exigidos para a obtenção do título de Doutora em Filosofia.

Orientador: Prof. Dr. Walter Alexandre Carnielli

Este exemplar corresponde à versão final da tese defendida pela estudante Mariana Matulovic da Silva, orientada pelo Prof. Dr. Walter Alexandre Carnielli, em 14/10/2013.

Campinas
2013

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Filosofia e Ciências Humanas
Cecília Maria Jorge Nicolau - CRB 8/338

M437d

Matulovic, Mariana, 1980-
Demonstrações na Algibeira : Polinômios como um Método Universal de Prova / Mariana Matulovic da Silva. – Campinas, SP : [s.n.], 2013.

Orientador: Walter Alexandre Carnielli.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Filosofia e Ciências Humanas.

1. Lógica. 2. Polinômios. 3. Lógica simbólica e matemática. 4. Lógica a múltiplos valores . 5. Determinismo (Filosofia). I. Carnielli, Walter Alexandre,1952-. II. Universidade Estadual de Campinas. Instituto de Filosofia e Ciências Humanas. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Demonstrations in the Algibeira : Polynomials as a Universal Method of Proof
Palavras-chave em inglês:
Logic
Polynomials
Logic, Many-valued
Logic, Symbolic and mathemathical
Determinism (Philosophy)
Área de concentração: Filosofia
Titulação: Doutora em Filosofia
Banca examinadora:
Walter Alexandre Carnielli [Orientador]
Itala Maria Loffredo D'Ottaviano
Marcelo Finger
Hugo Luiz Mariano
Jean-Yves Béziau
Data de defesa: 14-10-2013
Programa de Pós-Graduação: Filosofia

iv

UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS
INSTITUTO DE FILOSOFIA E CIÊNCIAS HUMANAS

A Comissão Julgadora dos trabalhos de Defesa de Tese de Doutorado, em sessão pública realizada em 14 de outubro de 2013, considerou a candidata MARIANA MATULOVIC DA SILVA aprovada.

Este exemplar corresponde à redação final da Tese defendida e aprovada pela Comissão Julgadora.

Prof. Dr. Walter Alexandre Carnielli

Profa. Dra. Itala Maria Loffredo Dottaviano

Prof. Dr. Hugo Luiz Mariano

Prof. Dr. Marcelo Finger

Prof. Dr. Jean-Yves Beziau

Abstract

This investigation aims to explore, in various aspects, the universal character of a powerful proof method, able to be used in classical and non-classical logics, in particular in propositional many-valued logics (deterministic and non- deterministic) in paraconsistent logics, in modal logics and in First Order Logic. This is the Method of Polynomial Rings, which can also be considered as an algebraic semantics, initially developed in (Carnielli 2005b). The method translates logical formulas into specific polynomials (usually finite, but sometimes infinite) with coefficients in finite fields, and transforms the problem of finding proofs in the search for solutions of systems of polynomial equations. This universality of the method enables the opening of several research lines, in particular the issue of truth-functionality and its generalizations. Other lines of research are: the possibilities of investigating alternative approaches of computational complexity, automatic theorem proving, heuristic methods in logic and correlations between algebra and logic. This study compares and analyzes the polynomial ring systems for systems with generalized truth-functionality, as in the case of non- deterministic semantic and even in systems where truth-functionality is lost, such as those many-valued systems reduced to bivalued by means of the so-called *Suszko reduction*. The method of polynomial rings, besides being a powerful and elegant apparatus in its apparent simplicity, is still a great teaching tool. Regarding classical logic, we define the polynomial ring for First Order Logic , based on a new domain that operates on sums and infinite products, called *domain of generalized series closed under products*. Finally, we evaluate the full potential of the method, especially in what concerns the question of obtaining a unifying feature that uses the same mathematical basis to translate different logical systems on similar algebraic varieties. Furthermore, we address the connections of the method with respect to algebraic logic (algebra of logic), and evaluate their perspectives.

Key-words: Logic, polynomial ring, proof method, deterministic and nondeterministic systems, algebrization, truth-functionality.

Resumo

O presente trabalho tem por objetivo explorar, em diversas vertentes, o caráter universal de uma ferramenta poderosa de prova, apta a ser utilizada em lógicas clássicas e não clássicas, em particular em lógicas multivaloradas proposicionais (determinísticas e não-determinísticas), em lógicas paraconsistentes, em lógicas modais e na Lógica de Primeira Ordem. Trata-se do Método de Prova de Anéis de Polinômios, que também pode, em princípio, ser visto do ponto de vista da semântica algébrica, desenvolvido inicialmente em (Carnielli 2005b). O método traduz fórmulas de uma lógica específica em polinômios (em geral finitos, mas podendo ser infinitos) com coeficientes em corpos finitos, e transforma o problema de se encontrar demonstrações no correlato algébrico da busca de soluções de sistemas de equações polinomiais. Esta universalidade do método possibilita a abertura de diversas linhas de pesquisa, sendo a questão da verofuncionalidade e suas generalizações uma delas. Outras linhas de pesquisa são: possibilidades de se investigar enfoques alternativos da complexidade computacional, prova automática de teoremas, métodos heurísticos em lógica e correlações entre álgebra e lógica. Este trabalho analisa e compara sistemas de anéis de polinômios para sistemas com verofuncionalidade generalizada, como no caso das semânticas não-determinísticas, e ainda em sistemas onde a verofuncionalidade é perdida, tais como em sistemas multivalorados reduzidos a bivalorados através da conhecida *redução de Suszko*. O método de anéis de polinômios, além de poderoso e elegante em sua aparente simplicidade, constitui ainda um ótimo instrumento pedagógico. Em relação à lógica clássica, definimos um anel de polinômios para a Lógica de Primeira Ordem, fundamentado em um novo domínio que opera com somas e produtos infinitos, o qual se denomina *domínio de séries generalizadas fechado por produtos*. Finalmente, procuramos avaliar todas as potencialidades do método, principalmente no aspecto inerente à questão de se poder pensar em uma característica unificadora na medida que utiliza o mesmo viés matemático para traduzir diferentes sistemas lógicos em variedades algébricas similares. Além disso, analisamos as interrelações do método com respeito a lógica algébrica (ou álgebra da lógica), e avaliamos suas perspectivas.

Palavras-chave: Lógica, anéis de polinômios, método de prova, sistemas determinísticos e não-determinísticos, algebrização, verofuncionalidade.

Sumário

Aos meus amados pais, Francisco e Soely.

Agradecimentos

Agradeço, primeiramente, a Deus, que iluminou meu caminho, me deu forças para prosseguir nessa jornada tão longa, que conhece todos os meus medos e anseios, que me consola e me ama. Enfim, te agradeço Pai pelas inúmeras vezes que você me enxergou melhor do que eu sou.

Agradeço aos meus pais, Francisco e Soely, que sempre abriram mãos dos seus sonhos para que eu e minhas irmãs pudéssemos realizar os nossos. Obrigada por todas as vezes em que pensei em desistir e vocês não deixaram. Por todas as vezes que caí, e vocês me levantaram. Por todas as vezes que ri, e vocês riram comigo. Agradeço a Deus, todos os dias, por ter me permitido ter vocês como meus pais. Pai, jamais esquecerei todas as palavras de força e fé que disseste durante a minha vida, principalmente quando eu não passei no vestibular e o senhor disse que pagaria, mesmo com tantas dificuldades, os anos de cursinho que eu precisasse para entrar na universidade. E à minha mãe, sempre forte, por ter me dando broncas no momento em que eu fraquejava, por abrir os meus olhos para os obstáculos da vida. Aos meus pais, minha eterna gratidão.

Como achar palavras para agradecer às minhas irmãs, Crislaine e Maria Claudia? Tenho tantas coisas a dizer mas não consigo, pois a emoção me impede. Somente essas duas pessoas sabem exatamente tudo que passei nesses doze anos entre graduação e doutorado. Todas as minhas tristezas e felicidades. Muito obrigada, Crislaine, por ser essa pessoa tão amiga, que sei que posso contar em todos os momentos, que cuidará sempre de mim. E a você, Maria Claudia, minha eterna "Nenê", só tenho a agradecer por todas as madrugadas que passou comigo durante minhas viagens a Campinas, por estar ao meu lado e me socorrer nos piores momentos da minha vida. Eu, simplesmente, sou louca por vocês.

Quero agradecer aos meus dois gatinhos, Vinícius e Gustavo, pela compreensão em relação à minha ausência. Sinto por não poder partilhar de mais tempo com vocês, de não acompanhá-los nessa fase de suas vidas. Mas saibam que o amor que sinto por vocês é, com certeza, igual ao de uma mãe.

Quero expressar meus eternos agradecimentos ao meu orientador Walter Carnielli, por seu constante apoio e confiança, por me assistir nas mais loucas e intempestivas decisões acadêmicas, pelas longas horas de trabalho em conjunto, por me encorajar a seguir em frente na procura do conhecimento, por todas as broncas proferidas de modo a me tornar uma verdadeira cientista. Muito obrigada.

Aos meus fiéis amigos e confidentes, Walter Carnielli e Juliana Bueno-Soler. Lembro-me como se fosse hoje a primeira vez que conversei com a Ju. Foi em 2007, no V Simpósio Internacional *Principia*. A empatia foi imediata e recíproca. Neste encontro, Deus me deu uma terceira irmã, aquela que estaria fisicamente comigo, quase que diariamente, em todos os meus momentos de desespero, de tristezas e alegrias mais profundas, de conquistas e derrotas, de fé

e desesperanças. Obrigada Ju, por ter sido essa amiga maravilhosa, por todas as nossas horas de estudos e conversas a respeito da lógica, por dividir comigo todas as suas conquistas e a sua família, pelos momentos compartilhados no San Petrus Bar, por ser uma amiga no sentido real e verdadeiro da palavra. Espero, apesar do meu ciúmes, que outras pessoas consigam ultrapassar a sua timidez e possam ter o privilégio de ser sua amiga. Ao amigo Walter, dentre todas as previsões (de bruxaria, é claro) que fez a meu respeito naquele primeiro encontro na sua casa, tem uma que eu jamais esquecerei: a de que eu seria muito feliz, tanto academicamente quanto pessoalmente. E, de fato, isto aconteceu, pois eu pude contar durante todos esse anos com uma pessoa que me acolheu não apenas como uma estudante, mas como filha, que me segurou forte e firme em todos os momentos que eu precisei. Amigo Walter, muito obrigada. Obrigada por ser essa pessoa íntegra, humana, carinhosa, companheira, amiga, fiel, brincalhona, desastrada, enfim, ser você. Ju e Walter, muito obrigada.

Quero também expressar meus agradecimentos às pessoas que colaboraram, de diversas maneiras e de forma influente, na realização desta tese: Aos professores Marcelo Esteban Coniglio e Itala Maria Loffredo D'Ottaviano, por seus ensinamentos; aos meus colegas, Juliana Bueno-Soler, Rodrigo de Alvarenga Freire, Leandro Suguitani, Rafael Testa, Samir Gorsky, Newton Peron, Edgar de Almeida, Pedro Mendes, Márcio Moretto, e aos demais amigos, pela amizade e pelas conversas acadêmicas. Aos membros da banca por terem levado a sério sua função com a maior competência e seriedade, e por suas sugestões e comentários muito pertinentes; à CAPES e ao portal de periódicos eletrônicos, que permite o acesso rápido e eficiente ao conhecimento científico; aos funcionários do Centro de Lógica, Epistemologia e História da Ciência, CLE; e a todos os demais não citados aqui mas os quais carrego em meu coração.

Gostaria de agradecer a uma pessoa que caminhou comigo, mesmo que por um tempo à distância, durante toda a minha jornada profissional: a minha amada "madrecita" Maria Augusta Rodrigueiro. Antes amiga, agora amiga e sogra. A vida me presenteou com essa dupla felicidade. Obrigada por me ensinar a ser uma profissional competente e íntegra, a tolerar minha ansiedade, por me aconselhar quando mais precisei, por me ajudar frente aos obstáculos da vida, por me permitir compartilhar com você a pessoa mais importante de nossas vidas: o seu filho.

A você, Franz Rodrigueiro, pretendo agradecer todos os dias das nossas vidas, te amando imensamente, te honrando e respeitando como homem e namorado, cuidando de você quando for preciso, tentando fazer sempre o máximo para te fazer feliz. Há uma música do Tom Jobim que, de certo modo, diz exatamente o que sinto por você. Ei-la aqui:

Pra que dividir sem raciocinar
Na vida é sempre bom multiplicar
E por A mais B
Eu quero demonstrar
Que gosto imensamente de você

Por uma fração infinitesimal,
Você criou um caso de cálculo integral
E para resolver este problema
Eu tenho um teorema banal

Quando dois meios se encontram desaparece a fração
E se achamos a unidade
Está resolvida a questão

Pra finalizar, vamos recordar
Que menos por menos dá mais amor
Se vão as paralelas
Ao infinito se encontrar
Por que demoram tanto os corações a se integrar?
Se infinitamente, incomensuravelmente,
Eu estou perdidamente apaixonado por você
(Aula de Matemática, de Tom Jobim)

Como eu sempre te digo, o meu amor por você é $2^{\aleph_0}$.

Somam-se-me dias.
Serei velho quando o for.
Mais nada.
Raiva de não ter trazido o passado
roubado na algibeira!

Fernando Pessoa

Introdução Geral

Algibeira, do árabe *al-jabira*, refere-se no português contemporâneo a um pequeno bolso onde se pode colocar moedas ou outras coisas pequenas e de valor. O termo álgebra tem a mesma origem de algibeira e, provavelmente refere-se a atividade de contar usando pequenas pedras que eram colocadas no bolso.[1]

Em algumas civilizações, como na Índia, já no século II, mecanismos formados por pedras que se deslocavam dentro de ranhuras eram usados como ábacos. Os polinômios na sua forma lúdica e aparentemente inocente, talvez sejam os objetos matemáticos que melhor lembrem as pedras primitivas usadas em cálculos.

No entanto, esta tese pretende mostrar que as expansões polinomiais com coeficientes em corpos finitos podem ter um grande poder de expressão e fundamentar um método bastante geral e amplo de representação da linguagem e dos métodos de prova em lógica.

Referimo-nos aqui não somente a lógica clássica mas também às lógicas modais, as lógicas multivalentes finitárias, a Lógica de Primeira Ordem e a certas lógicas que nem mesmo têm representação por meio de matrizes finitas.

De fato, discutiremos propriedades das representações polinomiais (ou polinômicas, termo que usaremos quando houver risco de confusão com o adjetivo "polinomial" usado na acepção de eficiência computacional), inclusive para as chamadas lógicas com semânticas não-determinísticas e para todas as outras lógicas acima, com exceção das lógicas modais que não serão tratadas nesta tese.

Dessa forma, os métodos que desenvolvemos podem ser pensados como ábacos abstratos que cabem em algum tipo de bolso.[2]

Diante disso, o método para provas automáticas de teoremas proposto por Walter Carnielli, em (Carnielli 2005b), denominado *Método de Provas por Anéis de Polinômios* é um mecanismo algébrico de provas, que traduz fórmulas lógicas de uma dada linguagem $\mathcal{L}$ em polinômios com coeficientes em apropriados corpos finitos e realiza deduções através de operações sobre esses polinômios.

O método também pode ser considerado como uma semântica algébrica, na qual a estrutura de polinômios reflete a estrutura das condições de valores de verdade para as fórmulas de lógica. Ele também pode ser visto como um método de prova (tal como o método de tableaux, que pode

[1] Curiosamente o termo cálculo também se refere a pedras.

[2] Não queremos, obviamente, que nosso título se confunda com o uso pejorativo "demonstrações **de** algibeira"

ser considerado como um sistema de prova teórica ou como um dispositivo de modelo teórico).

O objetivo desta tese é explorar o caráter universal do método, aplicando-o aos mais diversos sistemas lógicos, com exceção das lógicas modais, o que nos permite comparar, analisar e discutir características inerentes aos sistemas lógicos em questão.

Mas, por que seria interessante acrescentar mais um método de prova (ou semântico) para os sistemas lógicos? Atualmente, há várias abordagens subjacentes ao método geral de estudar as relações de consequências. Dentre elas, enfatizamos as seguintes questões:

- Eficiência;
- Universalidade;
- Relações com a álgebra;
- Heurística.

O método de anéis polinomiais torna-se interessante por aflorar questões em todas essas esferas. Isto é, em se tratando da eficiência do sistema, o método pode ser uma nova ferramenta na ilustração e resolução de problemas referentes à questão da eficiência computacional. Os fundamentos teóricos dos capítulos 1 e 3 desta tese proporcionaram o desenvolvimento de um software, PoLCa (Polynomial Ring Calculus), capaz de traduzir matrizes semânticas finito valoradas, determinísticas e não-determinísticas, em polinômios com coeficientes em um apropriado corpo.

Quanto à questão da universalidade, nosso trabalho mostra que o método de anéis de polinômios é aplicável nos mais diversos sistemas lógicos. Referimo-nos aqui não somente a lógica clássica mas também às lógicas modais, as lógicas multivalentes finitárias, a Lógica de Primeira Ordem e mais surpreendentemente, até certos sistemas lógicos não representáveis por meio de matrizes finitas

Em se tratando das relações com a álgebra, o uso de elementos simples e algébricos no método conduz a um possível reaproximação, e uma comunicação mais natural, entre lógica e álgebra, tal como ocorria nos trabalhos de George Boole, aproximação esta um tanto quanto perdida nas abordagens contemporâneas. Exploraremos esta conexão entre álgebra e lógica com mais detalhes no capítulo 1.

Além disso, o método pode ser visto como um dispositivo heurístico no sentido de descobrir novos sistemas lógicos ou novas propriedades de sistemas lógicos.

Diante deste contexto, iniciamos o primeiro capítulo com um apanhado histórico acerca do desenvolvimento dos polinômios, culminando com uma análise sobre as interrelações entre lógica e álgebra e, consequentemtente, sobre a algebrização da lógica. Além disso, introduzimos os conceitos primordiais a respeito do método de anéis de polinômios e delineamos alguns dos resultados já obtidos na aplicação do método ao Cálculo Proposicional Clássico e ao fragmento monádico da Lógica de Primeira Ordem. Esses trabalhos foram desenvolvidos por Walter Carnielli em uma série de artigos, dentre os quais destacamos:

- "A polynomial proof system for Łukasiewicz logics", (Carnielli 2001), 2001. Neste artigo, publicado no *Proceedings of the Second Principia International Symposium*, o autor desenvolve as principais ideias subjacentes ao cálculo de anéis de polinômios (CAP).

- "Polynomial ring calculus for many-valued logics", (Carnielli 2005b), 2005, é uma extensão mais detalhada do primeiro artigo.

- "Polynomial Ring Calculus for Logical Inference", (Carnielli 2005a), 2005. Neste artigo, uma versão polinômica para os sistemas paraconsistentes mbC and mCi são desenvolvidos. O interessante aqui é a inserção de um novo conjunto de variáveis, as variáveis ocultas, nas traduções desses sistemas.

- "Polynomizing: Logic Inference in Polynomial Format and the Legacy of Boole", (Carnielli 2007), 2007. Uma versão polinômica do fragmento monádico da lógica de primeira ordem é desenvolvida. O autor demonstra que qualquer função finita pode ser representada por polinômios com coeficientes em corpos finitos, usando para isto um caso particular do método de interpolação de Lagrange (teorema 3.1, p. 6);

- Em "Formal polynomials and the laws of form", (Carnielli 2009), 2009, o método pode ser visto como um dispositivo heurístico na descoberta de novas propriedades lógicas ou sistemas lógicos, tais como as half e quarter lógicas.

- Assim como no artigo anterior, em "Formal polynomials, heuristics and proofs in logic", (Carnielli 2010), 2010, o autor enfatiza a ideia de usar o método de polinômios como uma ferramenta heurística.

- "Polynomial Ring Calculus for Modal Logics: a new semantics and proof method for modalities", (Agudelo & Carnielli 2011), 2011. Walter Carnielli e Juan Carlos Agudelo desenvolvem o sistema modal S5 em uma versão polinômica.

O capítulo 2 é dedicado às Lógicas da Inconsistência Formal (LFIs), que internalizam as noções de consistência e inconsistência dentro da sua linguagem objeto por meio da introdução de novos operadores no escopo da linguagem, permitindo-nos assim separar as noções de contradição e inconsistência. Toda a fundamentação teórica na tese a respeito das LFIs advém do artigo "Logics of Formal Inconsistency", (Carnielli, Coniglio & Marcos 2007). Com o objetivo de empregar o método de anéis de polinômios em lógicas não-clássicas e paraconsistentes, avançamos no que já havia sido obtido em (Carnielli 2005a) para as lógicas mbC e mCi, definindo versões polinômicas para as seguintes LFIs: bC, Ci, mbCe, mCie, bCe, Cie e LFI1. Além disso, nossa contribuição também consistiu em melhorar as apresentações polinomiais para os sistemas mbC e mCi, que foram detalhadamente redefinidas.

A Lógica Proposicional Clássica é um exemplo paradigmático de uma estrutura semântica verofuncional e composicional. Para Gila Sher, em (Sher 2001), *composicionalidade* é uma noção metodológica: uma condição na estrutura semântica de uma dada linguagem, a qual está diretamente relacionada com a estrutura sintática dessa mesma linguagem. Em outras palavras, sintaticamente, cada fórmula bem formada de um dado sistema é unicamente determinada a partir de um número finito de expressões geradas por diversas aplicações dos operadores funcionais. Semanticamente a definição de verdade pode ser vista como uma imagem homomórfica da definição sintática, isto é, a cada sentença atômica é atribuída um único valor de verdade, T ou F, e para cada operador lógico há uma regra que determina, unicamente, o valor de verdade

de uma sentença formada por este operador, dados os valores de verdade de suas subfórmulas imediatas.

No caso específico da lógica clássica, sua linguagem completa contém uma coleção de conectivos m-ários que constroem fórmulas complexas, sendo as mesmas caracterizadas por tabelas de verdade com 2^m linhas, sendo que cada uma dessas linhas representa um possível valor de verdade atribuído às suas componentes sentenciais. Uma generalização das tabelas de verdade, para um número arbitrário de valores de verdade, está na construção de lógicas multivaloradas contendo "*graus de falsidade*" e "*graus de verdade*", ao invés da bivaloração usual.

Arnon Avron, em uma série de artigos tais como (Avron & Konikowska 2005), (Avron & Levi 2005), dentre outros, generaliza o conceito de uma estrutura multivalorada, de modo que uma atribuição de valor de verdade para uma fórmula complexa qualquer é concebida, indeterministicamente, a partir de um certo conjunto não-vazio de opções. Arnon Avron denominou essas estruturas por *Matrizes Não-Determinísticas*, ou *NMatrizes*.

Além disso, nos artigos (Avron 2007) e (Avron 2008), o autor representa uma boa parte das LFI's em forma de Nmatrizes. O foco do capítulo 3, representando nosso esforço original, está na aplicabilidade no método de anéis de polinômios em sistemas lógicos cujas semânticas são não-determinísticas. [3]

No capítulo 4, verofuncionalidade e anéis de polinômios continuam a ser os temas centrais. Nosso enfoque, na realidade, está na investigação da perda da verofuncionalidade em sistemas n-valorados que foram reduzidos em bivalorados, pela chamada Redução de Suszko. A Redução de Suszko, informalmente, nos diz que toda lógica tarskiana multivalorada pode ser caracterizada por uma lógica bivalorada. Na realidade Suszko ilustra sua proposição demonstrando como a lógica trivalorada de Łukasiewicz, $Ł_3$, pode ser tratada em função de uma semântica não-verofuncional bivalorada, na tentativa de criticar, acidamente, Łukasiewicz. Nossa contribuição foi definir, minuciosamente, os anéis de polinômios para os sistemas reduzidos pela Redução de Suszko, os quais foram apresentados em (Caleiro, Carnielli, Coniglio & Marcos 2005).

Diante do fato de que o método de anéis de polinômios mostrou-se apto para ser utilizado em sistemas lógicos clássicos, como no caso da Lógica Proposicional Clássica e do fragmento monádico da Lógica de Primeira Ordem, em não-clássicos, como nas LFIs, em sistemas com semânticas não-determinísticas, como no caso das Nmatrizes, verofuncionais e também não-verofuncionais, sistemas reduzidos pela Redução de Suszko, uma questão elementar a ser levantada seria a construção de uma versão polinômica para a Lógica de Primeira Ordem.

Nesse contexto, no capítulo 5 definimos a Lógica de Primeira Ordem (LPO) em uma versão polinômica, onde os quantificadores estão fundamentados em uma nova estrutura algébrica, denominada *domínio de séries generalizadas por produtos* (**SGP**), que nos permite operar com somas e produtos infinitos.

[3] Os principais resultados apresentados nesse capítulo serão publicados em um artigo, em janeiro de 2014, no Anais do LSFA - 8th Workshop on Logical and Semantic Frameworks, with Applications - sob o título: *Non-deterministic Semantics in Polynomial Format*.

Capítulo 1

O método de provas por anéis de polinômios

> "Algebra is the offer made by the devil to the mathematician...All you need to do, is give me your soul: give up geometry".
> (Michael Atiyah)

Durante os últimos anos, uma grande variedade de lógicas não-clássicas tem sido desenvolvida e, consequentemente, vários métodos de prova automática de teoremas foram propostos, tais como o cálculo de sequentes, o método de tablôs analíticos, etc. A maioria destes métodos estão fortemente relacionados as características inerentes e particulares de cada um desses novos sistemas lógicos. Apresentar implementações eficientes para tais cálculos especializados não é uma tarefa trivial, e isso acarreta dificuldades na manutenção e modificação desses sistemas para que estes possam se desenvolver com a mesma eficiência dos provadores da lógica clássica.

O método algébrico de provas de teoremas baseado na redução polinomial sobre finitos corpos que tratamos aqui não somente constitui um candidato a um competente método em termos de eficiência mas, ainda mais, cumpre as condições para um método natural de prova, nesse ponto análogo à dedução natural de Jaskowski e Gentzen.

Neste capítulo, expomos um breve contexto histórico acerca das descobertas algébricas que favoreceram o desenvolvimento dos polinômios. Além disso, uma análise a respeito da relação entre álgebra, lógica e consequentemente, sobre a algebrização da lógica é exibida. Em seguida, definimos o método para prova automática de teoremas proposto por Walter Carnielli, em (Carnielli 2005b), denominado *Método de Provas por Anéis de Polinômios*. Trata-se de um método algébrico de provas de teoremas baseado na redução polinomial sobre finitos corpos, particularmente apto para ser usado em lógicas finitárias multivaloradas e também para ser utilizado em certas lógicas não representáveis por matrizes finitas de valores de verdade, mas que possam ser caracterizadas por semânticas diádicas.

1.1 Polinômios como um artefato metodológico.

As ideias e concepções matemáticas, independente de haver ou não revoluções científicas na matemática, certamente evoluem no tempo. Já na matemática babilônica se encontram problemas e soluções que envolvem equações quadráticas. Em notação atual, são elas:

1. $x^2 + px = q$;
2. $x^2 = px + q$;
3. $x^2 + q = px$

Um fato interessante é que enquanto os egípcios e babilônicos operavam somas de segmentos com áreas ou de áreas com volumes, os gregos iniciavam uma fase em que a álgebra geométrica ocuparia o lugar desta antiga álgebra aritmética. Os processos algébricos mencionados no parágrafo precedente eram conhecidos como "*processos de aplicação de áreas*".

Após um longo período profundamente produtivo para a filosofia e para a geometria, com os trabalhos subjacentes às concepções filosóficas de Platão, Sócrates, Hipócrates, Eudoxus e Aristóteles, a álgebra só teve um desenvolvimento considerável com os trabalhos de Euclides de Alexandria.

"*Os Elementos*" de Euclides[1] é uma das obras mais importante da história da matemática, já que se trata de uma coleção que cobre toda a matemática elementar da época.

"*Os Elementos*" está dividida em treze livros, sendo os seis primeiros sobre geometria plana elementar, os três seguintes sobre a teoria dos números, o livro X sobre incomensuráveis e os três últimos versam sobre a geometria no espaço. O livro dois é o mais interessante para os nossos propósitos, pois nesta obra Euclides apresenta uma álgebra geométrica servindo para os mesmos fins da nossa álgebra simbólica. As equações lineares e quadráticas são resolvidas por construções geométricas, conduzindo à chamada "aplicação de áreas".

Todos os conceitos algébricos desenvolvidos antes de Euclides, inclusive as suas próprias contribuições, eram basicamente retóricos e um tanto quanto complicados de se entender. Diofanto, um matemático que viveu no século III a. C, contribuiu consideravelmente para tornar a álgebra mais simbólica, do que se chamaria "sincopada".

Em 1842, na obra "*Die algebra der Griechen*", Georg H. F. Nesselmann caracterizou três estágios lógicos da notação algébrica. São eles:

1. **Álgebra Retórica**: na qual as soluções de problemas são realizadas de modo escrito, sem abreviações ou símbolos, isto é, de modo argumentativo.
2. **Álgebra Sincopada**: Algumas abreviações são adotadas para quantidades recorrentes e para algumas operações específicas. No entanto, ainda a resolução é levada a efeito no modo argumentativo.
3. **Álgebra Simbólica**: neste tipo, as soluções aparecem quase que completamente compostas por uma abreviação matemática expressa por símbolos que, muitas vezes, não possuem conexões com as entidades as quais representam.

Diofanto escreveu três grandes obras: "*Números Poligonais*", "*Porismo*" e "*Aritmética*", sendo que existe apenas um fragmento da primeira obra e "*Porismo*" está perdido até hoje.

[1]Não podemos deixar de mencionar a tradução de "*Os elementos*" de Irineu Bicudo, sendo esta a primeira tradução completa para o português realizada a partir do texto grego. Para um estudo mais detalhado consultar "Os Elementos", tradução e introdução de Irineu Bicudo. São Paulo: Ed. Unesp, 2009

Já "*Aritmética*", sua obra mais importante, é composta por treze volumes, dos quais seis persistiram até nossos dias.

Para Eves em (Eves 1969), p. 159,

> The *Arithmetica* is an analytical treatment of algebraic number theory and marks the author as a genius is this field".

Essa obra contém 130 problemas algébricos de variados tipos, com equações do primeiro, segundo e até de terceiro graus.

O primeiro livro de "*Aritmética*" tem como tema norteador as equações determinadas por um elemento desconhecido, os demais com as equações do segundo grau e em alguns momentos, apresenta equações de níveis mais elevados, com dois e três elementos desconhecidos.

Do mesmo período de Diofanto datam os textos chineses mais antigos.

Datar os documentos matemáticos da China não é uma tarefa fácil, em decorrência da falta de registros autênticos, tanto em relação ao início da matemática chinesa quanto ao seu desenvolvimento. Estima-se, segundo Martzloff, em (Martzloff 2006), que os documentos mais antigos de que temos conhecimento são datados no período correspondente a 208 a. C a 8 d. C.

A obra "*Zhoubi suanjing*" é um dos principais documentos desse período, cujo tema central era a Cosmologia, na qual os autores (o livro parece ser o resultado de pesquisa de vários matemáticos desconhecidos) utilizam um tipo de numeração decimal. Além disso, esse autores sabiam como operar com frações (adicionar, subtrair, multiplicar e dividir) e conheciam o teorema que hoje denominamos por Teorema de Pitágoras.

Uma obra que é referência desse período é "*Jiuzhang suanshu*", conhecida pela denominação "*Nove Capítulos*". De acordo com Martzloff, em (Martzloff 2006), "*Nove Capítulos*" é uma referência obrigatória das obras chinesas, é o clássico dos clássicos.

Um dos capítulos mais significativo para o nosso interesse é o oitavo, por conter a resolução de problemas sobre equações lineares, cujas soluções podem ser tanto positivas quanto negativas. O último problema daquele capítulo envolve quatro equações com cinco elementos desconhecidos e algumas equações indeterminadas.

Entre 1247 e 1303 há um grande salto qualitativo no nível dos trabalhos chineses, levando em consideração a complexidade de seus algoritmos e a originalidade de seus resultados. Dentre as obras que marcaram essa época destacamos:

- "*The Ceyuan haijing*", 1248, de Li Zhi, no qual uma álgebra de frações racionais e polinômios generalizados (incluindo potências negativas de elementos desconhecidos) são desenvolvidos;
- "*The Yigu yanduan*", 1259, de Li Zhi, o qual é dedicado a construção algébrica e geométrica de 64 equações polinomiais de graus menores ou iguas a 2;
- "*The Suanxue qimeng*", 1299, de Zhu Shiyie, o qual descreve os rudimentos de uma álgebra polinomial;
- "*The Siyyan yujian*", 1303, Zhu Shiyie, que apresenta um procedimento de eliminação de elementos desconhecidos a partir de equações polinomiais com até quatro elementos desconhecidos.

Na vertente da matemática indiana, um dos maiores matemáticos do século XII foi, sem qualquer resquício de dúvidas, Bhaskara. Dentre suas principais contribuições destacamos a sua solução para a equação diofantina $x^2 - dy^2 = c$, onde c é um inteiro não-nulo e d um inteiro positivo, livre de quadrados. Tal equação diofantina recebeu mais tarde o nome de *Equação de Pell*.

Na sua principal obra "*Lilavati*", Bhaskara apresenta numerosos problemas sobre equações lineares e quadráticas, tanto determinadas quanto indeterminadas, progressões aritméticas e geométrica, radicais, tríades pitagóricas e combinatória.

Bhaskara morreu pelo fim do século XII e pelos vários séculos seguintes, nenhum desenvolvimento matemático significativo para o nosso propósito foi realizado na Índia.

Com a tradução árabe dos "*Siddhāntās*" por Al-Fazāri, por volta de 730 d. C, o mundo científico islâmico começou a se familiarizar com o chamado sistema indiano de numeração, o qual passou a ser utilizado cada vez mais pelo mundo árabe.

Em se tratando da matemática árabe, ou islâmica, temos as contribuições do matemático e astrônomo Muhammad ibn Mūusā al-Khwārizmī, que escreveu um tratado sobre álgebra e um livro a respeito dos numerais indianos.

Interessantemente, o segundo e mais importante livro de al-Khwārizmī denominado por "*Hisāb al-jabr wall-mugābala*" deu origem a um importante termo matemático, **álgebra**.

Nas palavras de Struik, (Struik 1948), p. 91,

> This algebra, of which the Arabic text is extant, also became known in the West through Latin translations, and they made the word "al-jabr" synonymous with the whole science of "algebra", which, indeed, until the middle of the Nineteenth Century was nothing but the science of equation.

A obra "*Hisāb al-jabr wall-mugābala*" contém uma discussão direta e elementar da resolução de equações lineares e quadráticas, mas sem qualquer formalismo algébrico, nem mesmo o Sincopado de Diofanto. Segundo Boyer, (Boyer & Merzbach 1991), o livro se inicia com uma breve introdução a respeito do princípio posicional dos números e em seguida, no decorrer dos seus seis capítulos, apresenta a resolução dos seis tipos de equações formadas com as três espécies de quantidades: raízes, quadrados e números.

Al- Karkhi (ou Al-Karagi), por volta de 1029, interessou-se pela álgebra de al-Khwārizmī. Como ele era um discípulo árabe de Diofanto, seus trabalhos refletem a utilização do simbolismo sincopado à la Diofanto nas concepções algébrica apresentadas por al-Khwārizmī. Apesar da sua preocupação com equações quadráticas, o foco de interesse de al- Karkhi estava nas equações de graus superiores a 2. São atribuídas a al- Karkhi as primeiras soluções numéricas das equações da forma $ax^{2n} + bx^n = c$, no qual apenas raízes positivas eram consideradas.

Já o persa Omar Khayyan (1050 - 1122) escreveu uma "*Algebra*" que contém uma investigação sistemática de equações cúbicas, cujas raízes são determinadas pela intersecção de duas secções cônicas, assim como faziam os gregos.

Na Idade Média Alta, as primeiras cidades comerciais e poderosas surgiram na Itália, e a relação entre essas cidades e o mundo árabe e o norte tornou-se cada vez mais constante e intenso. Dentre essas cidades temos Veneza, Milão, Genova e Pisa.

O primeiro mercador ocidental que merece destaque por suas contrinuições para a matemática foi Leonardo de Pisa (1180- 1250), conhecido também por Fibonacci. Sua obra "*Liber*

Abaci" é um tratado completo sobre métodos e problemas algébricos em que o uso de numerais hindu-arábicos é recomendado.

No decorrer dos quinze capítulos de "*Liber Abaci*", Fibonacci explica o sistema de numeração que ele irá utilizar, apresenta novos métodos de cálculo com números inteiros e frações, exibe o cálculo de raízes quadradas e cúbicas e expõe métodos para a resolução de equações quadráticas.

As cidades italianas continuaram a revelar competência na matemática depois de Leonardo de Pisa. No século XV, os mestres de cálculos dessas cidades tinham domínio pleno das operações aritméticas, incluindo em relação aos números construtíveis.

Dentre os matemáticos importantes dessa época destacamos um exímio algebrista, que é conhecido e titulado como um dos maiores matemáticos italianos dos séculos XIV e XV: Antonio de' Mazzinghi.

Segundo Raffaela Franci, em (Franci 1988), as três maiores enciclopédias da matemática medieval citam o tempo todo os trabalhos de Mazzinghi e o clamam como um algebrista de competência inegualável. As obras em questão são: "*Patalino 573*" da Biblioteca Nacional de Florença, "*Ottoboniano latino 3307*" da Biblioteca do Vaticano e "*L. IV 21*" da Biblioteca Municipal de Siena.

Franci, em (Franci 1988), narra um fato muito curioso a respeito da vida de Mazzinghi. Dizem que quando Paolo dell'Abaco (um grande matemático da época) faleceu, ele determinou em seu testamento que todos os seus livros fossem doados ao matemático mais habilidoso e instruído de Florença. Para tanto foi necessário uma comissão de quatro mestres em matemática, os quais após uma discussão que perdurou por 5 anos, decidiram escolher Antonio de' Mazzinghi. Nas palavras da própria autora, p.241,

> In his will Paolo directed that all his astrological books and instruments be placed in a case until a committee of four masters close the most learned mathematician in Florence. After a long discussion (while ran five years) among the judges, the books and instruments were given to the young Antonio.

Antonio de' Mazzinghi escreveu muitos tratados em aritmética e geometria, mas dentre eles o mais importante foi intitulado "*Fioretti*", uma grande obra em álgebra. Em "*Fioretti*", o autor apresenta operações com monômios e polinômios, regras para as resolução de nove tipos de equações e diversos outros problemas resolvidos com ferramentas algébricas, que antes eram solucionados geometricamente.

É importante lembrarmos que neste período, o elemento desconhecido e suas potências eram representados por meio de palavras, assim como a apresentação das equações e das regras que as solucionam. Diante disso, em um simbolismo moderno, na primeira parte de seu tratado Antonio de' Mazzinghi apresenta algumas regras para a multiplicação entre termos da álgebra, tais como:

- $x.x = x^2$;
- $x.x^2 = x^3$;

e assim por diante.

Além disso, ele também introduz a divisão do elemento desconhecido com a sua potência (até a potência 6), isto é, apresenta as frações $\frac{1}{x}, \frac{1}{x^2}, ..., \frac{1}{x^6}$.

Na segunda parte do seu tratado, existem nove tipos de equações com suas respectivas regras de resolução. Na álgebra renascentista as equações eram formadas pela igualdade de dois polinômios em que:
(i) quando em cada lado da igualdade havia um monômio, a equação era dita *simples*;
(ii) caso contrário, ela era denominada *composta*.

Em um simbolismo atual, as noves equações eram as seguintes:

1. $ax = c$;
2. $ax^2 = c$;
3. $ax^3 = c$;
4. $ax^4 = c$;
5. $ax^5 = c$;
6. $ax^6 = c$;
7. $ax^2 = bx + c$;
8. $ax^2 + bx = c$;
9. $ax^2 + c = bx$;

Um pupilo de Antonio de' Mazzinghi, denominado Domenico d'Aghostino, afirmou que cópias dos tratados de Mazzinghi estavam em posse do abacista Lorenzo do Bagio. Infelizmente, nenhum dos numerosos manuscritos dos séculos XIV e XV a respeito da álgebra fazem menção a qualquer trabalho de Antonio de' Mazzinghi.

Não há dúvida que Antonio de' Mazzinghi foi um matemático de qualidade ímpar em métodos algébricos, já que a grande maioria dos matemáticos dessa época, tal como Leonardo de Pisa, evitavam utilizar cálculos algébricos e optavam por uma resolução mais geométrica.

Com o advento da imprensa, século XV, livros começaram a ser publicados para o ensino da aritmética prática. Um dos livros matemáticos mais importante desse período foi "*Summa de Arithmetica, Geometria, Proportioni et Proportionalitá*", 1494, de Luca Pacioli.

Durante as décadas seguintes a álgebra e a aritmética calculacional foram os temas prediletos dos matemáticos, aqui incluindo Cardano, del Ferro, Tartaglia e Bombelli. E, como o pensamento filosófico muitas vezes reflete a tendência do pensamento científico, a admiração pelo raciocínio quantitativo foi crescente entre os filósofos da época.

François Viéte (1540- 1603) foi um dos primeiros a representar números por letras utilizando para tanto as vogais para denotar uma quantidade supostamente desconhecida ou indeterminada, e as consoantes para explicitar grandezas ou números supostamente conhecidos. A álgebra de Viéte ficou conhecida como *Álgebra Speciosa*.

De Newton e Leibniz até Laplace (1749), quase todo o desenvolvimento da matemática centrou-se em torno do cálculo diferencial integral e suas aplicações e no desenvolvimento da

probabilidade. A dependência entre o cálculo e a álgebra é particularmente notória na obra de Newton, cujo cálculo é praticamente um tratamento da álgebra de polinômios infinitos.

O século XVIII assisitiu ao surgimento de um dos matemáticos mais produtivos de todos os tempos: Leonhard Euler (1707- 1783). Dentre as contribuições de Leonhard Euler destacamos seus trabalhos com polinômios infinitos (os quais serão trabalhados no capítulo 5), a introdução da função gama, a relação entre o cálculo diferencial de Leibniz e o método das fluxões de Newton e a resolução de equações diferenciais com a utilização do fator integrante.

O século XIX foi marcado por uma mudança considerável em relação à matemática, em que o foco de desenvimento foi modificado. Na linha divisória entre os século XVIII e XIX encontramos a figura majestosa de Carl Friedrich Gauss (1777 - 1855). Suas primeiras descobertas foram publicadas em sua dissertação, onde exibe a primeira prova rigorosa do "teorema fundamental da álgebra", o qual mostra que qualquer equação algébrica de grau n com coeficientes reais tem n raízes.

A lógica, como um campo separado de estudo, tem suas raízes nos silogismos de Aristóteles. A aplicação de técnicas matemáticas na lógica deve a muitos esforços, incluindo os de Leibniz, e é revivida e fundamentada nas obras de Boole, em meados do século XIX.

George Boole (1815- 1864) pode ser visto com um dos maiores lógicos de todos os tempos. O marco principal de seu trabalho está na aplicação de métodos da emergente *álgebra simbólica* em lógica. O olhar algébrico decorrente do enfoque de Boole permitiu formular métodos de simplificações para uma enorme gama de problemas, com grande capacidade unificadora.

Estes métodos foram descritos em duas obras:

1. *"The Mathematical Analysis of Logic"*, de 1847, onde Boole apresenta uma abordagem algébrica para a lógica Aristotélica.

2. *"The Laws of Thought"*, de 1854, sua obra principal, em que Boole esforça-se para corrigir e aperfeiçoar o *"The Mathematical Analysis of Logic"*.

Boole usava letras simples, como por exemplo o x, para representar classes de objetos, sendo que o algarismo 1 representava o *Universo*, o qual compreende toda a classe de objetos concebíveis, existentes ou não. Havia também a classe do *Vazio*.

A operação da *adição* foi introduzida como a união de conjuntos ditos disjuntos. Boole apresentou algumas leis que regiam a adição, como a *lei da comutatividade*, $x+y = y+x$ e a *lei distributiva*, $z(x+y) = zx+zy$. Já a operação da *multiplicação* foi definida como a intersecção de duas classes, a qual obedecia às seguintes leis:

- Comutatividade: $xy = yx$.

- Lei do índice ou lei da idempotência: $x^2 = x$.

Além dessas leis, Boole assumiu que $x + x = 0$ implica que $x = 0$, e a existência do inverso aditivo. No entanto, ele não considerou a existência do inverso multiplicativo. A *lei da idempotência* ou *lei do índice* ocupava uma posição central na teoria de Boole, pois para uma lei fundamental da metafísica, $x^2 = x$, o que tínhamos na realidade era consequência de uma lei do pensamento. Em outras palavras, $x^2 = x \Rightarrow x^2 - x = 0 \Rightarrow x(x-1) = 0$, representa que a conjunção de "x" e "não-x" é impossível, isto é, a lei da não-contradição.

Um fato muito importante a ser enfatizado neste momento é que em 1847, em "The Mathematical Analysis of Logic", Boole aceitou a generalização da lei do índice, isto é, $x^n = x$. No entanto, em 1854, em "The Laws of Thought" tal generalização foi rejeitada. Tudo isso ocorreu em virtude do fato de que se $x^n = x$, então particularmente, $x^3 = x$. Logo, $x^3 - x = 0 \Rightarrow x(x^2 - 1) = 0$. Assim, tanto $x = 1$ quanto $x = -1$ são raízes dessa equação. Mas aqui ocorre um problema, pois (-1) não é válido na teoria desenvolvida por Boole, pois tal número não obedece a lei do índice, ou seja, $(-1)^2 \neq (-1)$.

O fato que impediu Boole de avançar foi não notar que, ao se generalizar a lei do índice para $x^n = x$, deve-se substituir uma lei anterior $x^m = x$ (para $m \neq n$) pela nova lei, e não obrigatoriamente manter ambas. Em outras palavras, sem correr o risco de anacronismo, podemos dizer que a ausência da noção de corpos algébricos impedia Boole de ver que se poderia realizar a álgebra da lógica em universos distintos.[2]

Assim como Boole, em 1847 Augustus De Morgan (1806- 1871) publicou um livro de lógica intitulado *"Formal Logic"*. Em uma perspectiva completamente diferente da de Boole, a abordagem de De Morgan tencionava analisar a lógica aristotélica em seus componentes mínimos e desenvolver, a partir desses componentes um novo sistema. Infelizmente esta obra foi totalmente ignorada, pois De Morgan não conseguiu desenvolver uma álgebra equacional da lógica em função da omissão para um símbolo que representasse a igualdade.

Apesar disso as contribuições de De Morgan foram memoráveis e continuam a ser utilizadas até hoje, como por exemplo, na formulação das leis que levaram o seu nome, as Leis de De Morgan.

Um estudante de De Morgan, William Stanley Jevons (1835- 1882), publicou em 1864, na obra intitulada *"Pure Logic"*, uma abordagem alternativa para o sistema proposto por Boole, já que para ele a operação de adição desenvolvida por Boole deveria ser substituída.

Jevons defendia que a operação correta de adição para o sistema de Boole deveria ser uma operação *inclusiva*, de união total, a qual conduziria à seguinte lei aditiva: $x + x = x$. Tal mudança, no entanto, destruiria o sistema booleano e por isso, Boole ignorou completamente qualquer tipo de mudança sugerida por Jevons. Uma das maiores contribuições de Jevons, além dessa constatação a respeito da adição, foi o desenvolvimento do moderno sistema de Álgebra Booleana. Independentemente de Jevons, Charles Sanders Peirce também chegou à mesma conclusão a respeito da substituição da operação de adição no sistema de Boole.

Não poderíamos deixar de lado o matemático alemão Ernst Schröder (1841- 1902). Schröder resumiu e ampliou os trabalhos iniciados e deixados por Boole, De Morgan e Peirce. Em sua obra mais famosa, *Vorlesungen über die Algebra der Logik*, ele apresenta a sua formulação da Lógica de Boole, considerando a adição e a multiplicação como operações lógicas e destaca o caráter dual que as envolve. Além disso, Schröder introduz os símbolos Σ e Π como operadores análogos aritméticos da conjunção e disjunção.

A introdução de métodos algébricos abstratos em diferentes sistemas matemáticos ajudou a unificar desenvolvimentos em análise, teoria dos números, teoria das equações, geometria, etc. O final do século XIX foi marcado, principalmente, pela introdução de uma nova linguagem teórica fundamentada na nascente teoria dos conjuntos e pelo surgimento de métodos infinitários de

[2]Distintos, obviamente, das álgebras de Boole.

prova, cujo objetivo era suprimir ou minimizar conteúdos computacionais tão comumente usados nas argumentações matemáticas desta época.

No entanto, essas mudanças deram origem a uma forte preocupação a respeito da possibilidade de tais métodos serem apropriados e significativos para a matemática. A descoberta dos *paradoxos* decorrentes do uso excessivamente ingênuo dessa nova linguagem, conduziram a preocupações ainda mais importantes, como a verificabilidade da consistência desses métodos.

Tudo isto desencadeou uma crise nos fundamentos da matemática e uma busca incessante para uma base matemática mais segura e certa foi iniciada. As ameaças definicionais colocadas pela descoberta dos paradoxos originaram acaloradas batalhas ideológicas entre os pesquisadores de várias escolas do pensamento deste período.

Em palestras apresentadas em 1922, David Hilbert lançou sua *"Teoria da Prova"*, *Beweistheorie*, cujo objetivo era justificar a utilização de métodos modernos em provas e acabar, de uma vez por todas, com a crise dos fundamentos da matemática. Assim, segundo Hilbert, teríamos que representar o sistema matemático infinitário por meio de sistemas formais, pelo fato deles estabelecerem uma linguagem formal fixa e regras de inferências precisas. Logo, as provas desses sistemas seriam finitas e consistentes.

Sendo assim, para Hilbert era necessário uma formalização de toda a matemática de um modo axiomático no qual deveria ser demonstrado, por métodos finitários, que esta axiomatização era de fato consistente. Diante disso, o caráter epistemológico do raciocínio finitário produziria a justificação matemática tão almejada naquele momento de crise. Como se sabe, os famosos teoremas de incompletude de Kurt Gödel representaram um enorme obstáculo a esse projeto.

Preocupados com os objetivos do Programa de Hilbert, o qual buscava fixar a matemática em uma base segura e consistente, tanto Gerhard Gentzen (1934), na obra *Untersuchungen über das logische Schliessen* ("Investigations into Logical Deduction") quanto Stanislaw Jaskowski (1934), em *On the Rules of Suppositions in Formal Logic*, forneceram, ao mesmo tempo e de modo independente, uma abordagem mais natural para o pensamento formal, por meio da dedução natural.

Toda essa inquietação levou a uma investigação mais aprofundada a respeito das propriedades estruturais das provas formais. Este estudo é o cerne das pesquisas relacionadas à chamada teoria da prova.

A teoria da prova é uma área da matemática que estuda os conceitos de *prova matemática* e analisa a estrutura geral das provas matemáticas. Diante disso, a noção de *prova* desempenha um papel fundamental dentro desta teoria.

De acordo com (Buss 1998), cabe à teoria da prova:

1. Formular sistemas da lógica e conjuntos de axiomas apropriados para formalizar provas matemáticas e, consequentemente, caracterizar quais resultados matemáticos são consequências de certos conjuntos de axiomas.

2. Analisar e estudar a estrutura de provas formais.

3. Examinar o tipo de informação adicional que pode ser extraído das provas além da própria verdade do teorema a ser provado.

4. Avaliar qual é a melhor construção de provas formais, isto é, que tipos de provas são mais adequadas para serem aplicadas em dispositivos computacionais.

O século XIX foi marcado pela incessante incorporação de métodos algébricos na lógica. Seria natural então fundamentar uma *teoria algébrica de provas*. Uma tal teoria analisaria os procedimentos de prova que de alguma forma tiraria proveito de métodos, resultados e maquinaria algébricos. A ideia, portanto, é usarmos diretamente o método algébrico para a obtenção de provas e propriedades lógicas. Este ponto de vista é herdado, como vimos, dos trabalhos de Leibniz, Boole, De Morgan, Peirce e Hilbert.

A matemática contemporânea tem resultados profundos, iniciados com David Hilbert, relacionando soluções de equações polinomiais com ideais de anéis polinomiais em várias variáveis.

Um deles é o famoso *Nullstellensatz*, devido a Hilbert em 1893 ("teorema dos pontos nulos"), um teorema em geometria algébrica que relaciona variedades e ideais em anéis de polinômios sobre corpos algebricamente fechados.

Outro clássico é o "teorema da base" de Hilbert , que mostra que todo ideal no anel de polinômios multivariados sobre um anel Noetheriano é finitamente gerado. Isso pode ser traduzido em geometria algébrica da seguinte forma: todo conjunto algébrico sobre um corpo pode ser descrito como o conjunto de raízes comuns de um número finito de equações polinomiais. Hilbert provou, em 1890, este teorema de uma forma não-construtiva: seu método não dá um algoritmo para produzir um número finito de polinômios de base para um determinado ideal. Ele só mostra, por um processo de redução ao absurdo, que tais polinômios devem existir. Pode-se, contudo, determinar polinômios de base utilizando o chamado método de bases Gröbner.

Uma base de Gröbner B para um sistema de polinômios A é um sistema de equivalência que possui propriedades úteis, por exemplo, tais que um outro polinômio é uma combinação daqueles da base em A sse o resto com respeito a B é nulo (aqui, o algoritmo da divisão exige uma ordem de um certo tipo sobre os monômios). Além disso, o conjunto de polinômios em uma base de Gröbner têm a mesma coleção de raízes dos polinômios originais.

Embora as bases de Gröbner possam ser usadas na resolução do sistema de equações algébricas e também ser utilizadas para investigar a complexidade de provas, isto tudo não é, certamente, mais do que arranhar a superfície da potencialidades dos métodos algébricos de provas e, mesmo assim restrita a lógica clássica.

O método de polinômios estudado nesta tese aponta para um método geral de prova para lógicas polivalentes (determinísticas e não determinísticas, como iremos esclarecer, envolvendo uma grande gama de sistemas lógicos) que de algum modo são semelhantes às intuições do *Nullstellensatz*, e consequentemente relaciona-se também com o cálculo de Gröbner. Não deixa de ser interessante notar que, o mesmo Hilbert que funda a teoria da prova e inaugura a geometria algébrica, não nota explicitamente as conexões entre as duas áreas.

Muito provavelmente o desinteresse de Hilbert por esta conexão tenha resultado de sua maneira de abordar a lógica, desarticulada da álgebra da lógica. Vejamos, com mais detalhes, o desenvolvimento da álgebra da lógica.

1.2 Desenvolvimento da visão algébrica da lógica.

A lógica algébrica surgiu como uma subdisciplina da álgebra, buscando refletir (no espelho da álgebra) teoremas da lógica matemática.

É importante salientarmos que o que se denomina "lógica algébrica" é a variante do raciocínio lógico obtido através da manipulação de equações com variáveis livres. Existe sempre o risco de se confundir esta noção com "álgebra da lógica", " algebrização de lógicas " e "semântica algébrica". As distinções são muito técnicas e muito sutís para se tratar neste trabalho, mas podemos pelo menos dizer que, na sua contraparte algébrica, nosso trabalho pode ser visto como inserido na tradição da "lógica algébrica".

Historicamente, conforme já exposto, George Boole com seu *Mathematical Analysis of Logic: Being an Essay Towards a Calculus of Deductive Reasoning*, (Boole 1951), é tido como seu fundador, tendo se aproximado da lógica de uma perspectiva completamente diferente, apresentando a lógica aristotélica sob o manto da álgebra simbólica.

Mas a lógica algébrica é, talvez, a abordagem mais antiga para a lógica formal, começando com uma série de notas que G. Leibniz escreveu em 1680, alguns dos quais somente foram publicados no século 19, traduzidos para o inglês por Clarence Lewis. Segundo diversas fontes (sem pretender aqui nenhuma contribuição histórica) a contribuição madura de Leibniz estava presente em sua *Generales Inquisitiones de Analysi Notionum et Veritatum*, que só foi publicada na edição de L. Couturat em 1903.

A esse respeito, a conexão entre álgebra e lógica é semelhante à que ocorre em áreas como geometria algébrica e topologia algébrica, onde os principais teoremas e construções são algébricos em sua natureza, mas as principais intuições subjacentes são, respectivamente, geométrica e topológica.

A investigação em lógica algébrica procede em duas vertentes diferentes, mas muitas vezes relacionadas. Primeiro tenta-se investigar a essência algébrica das construções da lógica, na esperança de ganhar mais conhecimento que se poderia acrescentar à sua compreensão. Pode-se, por outro lado, estudar certas particulares estruturas algébricas (ou simplesmente álgebras) que surgem no decorrer da primeira espécie de investigação como objetos de interesse em seu próprio direito e passar a discutir questões que naturalmente surgem independentemente de qualquer conexão com a lógica. Contudo, muitas vezes esses resultados puramente algébricos têm um impacto sobre a lógica.

Ao lado de Leibniz e Boole, Charles Peirce foi outra figura de grande estatura na área. Peirce começou sua investigação sobre a álgebra da lógica no final da década de 1860, chegando de forma independente à mesma conclusão que Jevons tinha antes chegado, a saber, que é necessário substituir o funcionamento parcial da adição que propunha Boole pela operação total de união. Em seu importante artigo de 1880, "On the Algebra of Logic", Peirce rompe com a semântica aristotélica (semântica que não admite classes vazias) introduzindo uma semântica moderna para a lógica. Peirce usou a expressão *algebra booleana* para denotar o trabalho desenvolvido por Boole.

Inspirado pelo trabalho de De Morgan de 1860, Peirce também considerou uma série de outras operações naturais sobre relações. Ao empregar uniões, possivelmente infinitas, sem restrições, denotadas por Σ, e interseções, possivelmente infinitas, sem restrições, denotado por

Π, Peirce introduziu os quantificadores em sua álgebra da lógica. Embora De Morgan receba o crédito pela introdução do conceito de relações, Peirce é considerado o verdadeiro criador da teoria das relações.

A. Whitehead e B. Russell, com sua visão logicista inerente ao famoso *Principia Mathematica*, rejeitaram a álgebra em sua abordagem lógica, com suas fórmulas e anotações emprestadas da álgebra comum das equações, em favor da abordagem desenvolvida por G. Frege (e com influências de G. Peano), ou seja, preferiam pensar em termos de conectivos lógicos, símbolos de relação e quantificadores.

Tal posição se reflete também na obra menos conhecida de Whitehead, seu *Treatise of Universal Algebra*, (Whitehead 1898) uma profunda investigação dos vários sistemas de raciocínio simbólico relacionados à álgebra ordinária, seguindo a Teoria dos Quatérnions de Hamilton, o Cálculo de Extensões de Grassmann e as idéias de Boole em Lógica Simbólica.

Hilbert de certa forma concordou com esta abordagem, e a álgebra da lógica caiu em desuso até 1941, quando A. Tarski retornou à álgebra das relações de Peirce como apresentado no livro de E. Schröder, *Vorlesungen über die Algebra der Logik*.

Mas, anteriormente a Tarski, o lógico norueguês Thoralf Skolem já inaugurara os primeiros esforços na tradição algébrica da lógica, diferente da tradição Frege-Russell-Hilbert e que seria mais tarde celebrizado por Tarski.

Os três primeiros trabalhos de Skolem em lógica (datados de 1913, 1919 e 1920) pertencem à tradição algébrica que ele empreendeu a partir dos volumes da obra de Schroder, *Vorlesungen über die Algebra der Logik*, sendo que o artigo de 1913, (Skolem 1913), começa com um enfoque admiravelmente conciso da abordagem algébrica da lógica em termos de teoria da reticulados.

Tarski reviveu, então, a álgebra das relações em seu artigo de 1941, *On the Calculus of Relations*, (Tarski 1941), primeiramente esboçando uma lógica formal que permitia a quantificação sobre ambos, elementos e relações, e então dedicando-se a um estudo mais detalhado das fórmulas livres de quantificadores, que envolviam apenas as variáveis de relação. Depois de apresentar uma lista de axiomas que, obviamente, valia para a álgebra de relações, tal como apresentado por Schröder, ele provou que esses axiomas permitiam reduzir fórmulas livres de quantificadores de relação em equações.

Na verdade, o poder expressivo da álgebra de relações é exatamente equivalente ao da lógica de primeira ordem com apenas três variáveis. No entanto, se o que se deseja é formalizar a teoria dos conjuntos com, por exemplo, o axioma do par nas álgebras de relações (ou seja, através do cálculo de relações) então pode-se reduzir o número de variáveis a três variáveis, e por isso é possível expressar qualquer sentença de primeira ordem de tal teoria por uma equação.

Evidencia-se, dessa forma, o imenso poder da mera relação de igualdade para a lógica, traço que será de importância fundamental para nosso trabalho, onde a noção de demonstrar se reduz à existência de soluções para sistemas de polinômios sobre corpos finitos, mas isso generalizado para uma ampla família de lógicas (e não somente para o caso clássico).

M. Stone, autor da talvez maior façanha algébrica que auxilou o renascimento da lógica algébrica nas mãos de Tarski, perguntava-se sobre a estrutura de uma álgebra booleana arbitrária. Pergunta esta que ele mesmo respondeu, demonstrando que toda álgebra booleana é isomorfa a uma álgebra booleana de conjuntos. Em seu trabalho sobre álgebras booleanas, Stone notou

uma certa analogia entre núcleos de homomorfismos e os ideais estudados na teoria dos anéis, e isso o levou a dar o nome de "ideal" a esses núcleos. Pouco tempo depois, ele descobriu também uma tradução entre álgebras de Boole e anéis booleanos; sob esta tradução, os ideais de uma álgebra booleana correspondem precisamente aos ideais do anel booleano associado.

Nos anos entre 1948-1952, Tarski, (Henkin & Tarski 1961) juntamente com seus estudantes, criou as álgebras cilíndricas como uma contraparte (em termos de lógica algébrica) para a lógica de primeira ordem, e Halmos em (Halmos 1962) introduziu as álgebras poliádicas com a mesma finalidade.

As álgebras cilíndricas, são essencialmente álgebras booleanas equipadas com operações unárias $C(x)$, ditas cilíndricas, que se destinam a capturar as propriedades tidas como essenciais dos quantificadores existenciais $(\exists x)$.

Contudo, como Halmos, em (Halmos 1962) observou, essas novas lógicas algébricas tendem a se concentrar em investigar até que ponto se capturara lógica de primeira ordem e em seus aspectos algébricos universais, como axiomatizações e estrutura de teoremas, mas oferecem pouca intuição sobre a natureza da lógica de primeira-ordem que inspirou sua criação.

Mesmo se nos voltarmos às lógicas multivalentes, o análogo das álgebras de Boole seriam as MV-álgebras, basicamente dedicadas às lógicas de Łukasiewicz, as álgebras de Post, de Kleene, etc., mas as dificuldades para se produzir uma contraparte algébrica para lógicas multivalentes em geral, e em especial para lógicas paraconsistentes (como por exemplo discutido em (Bueno-Soler & Carnielli 2005)) são imensas.

Um ponto recorrente na nossa investigação é o caso da distinção entre anéis booleanos e álgebra de Boole. Uma confusão comum consiste em se deixar enganar pela interdefinibilidade entre tais estruturas; de fato, embora álgebras de Boole e anéis booleanos sejam estruturas matemáticas interdefiníveis, não são estruturas isomorfas (mas constituem categorias isomorfas). Deve-se notar que a definição de isomorfismo exige que estruturas isomorfas compartilhem a mesma assinatura (linguagem), o que não ocorre neste caso.

Mas, mais importante ainda, a interdefinibilidade se mantém apenas no caso bivalente, as coisas mudam drasticamente no caso n-valente: os anéis booleanos se generalizam de maneira imediata e natural via anéis de polinômios sobre corpos de Galois, o que não acontece com as as álgebras de Boole.

Decididamente, a álgebra da lógica de Boole não é a álgebra booleana, tal como modernamente concebida, pois Boole não trabalhou, por exemplo, com uma álgebra de dois elementos. O que seria tal álgebra da lógica, aventuramo-nos neste trabalho a conjecturar, seria algo muito mais próximo ao Cálculo de Anéis de Polinômios desenvolvidos nesta tese: testemunhas a nosso favor são o tratamento natural que se pode dar para as lógicas finito-valentes em geral, determinísticas e não-determinísticas (veja capítulo 3, seção 3.3), e mesmo para suas versões bivaloradas não-verofuncionais (veja capítulo 4, seção 4.3), e ainda para as lógicas paraconsistentes, que sequer são algebrizáveis pelos métodos tradicionais (veja capítulo 2). O tópico mais complexo deste trabalho, do ponto de vista matemático, é o tratamento via anéis de polinômios para a lógica de primeira ordem. Mas mesmo nesse caso, tratando-se liberalmente polinômios infinitos com um certo olhar heurístico, como fazia Euler, fica evidente a naturalidade do método, e seu sabor algébrico muito mais palatável que as álgebras cilíndricas. Uma nova maneira de se olhar

para a álgebra da lógica? Talvez. Mas isso é tarefa reservada ao futuro, conforme exposto no capítulo 6.

1.3 O cálculo de anéis de polinômios

O cálculo de anéis de polinômios (CAP) consiste basicamente em traduzir fórmulas de uma dada lógica $\mathcal{L}$ em expressões polinomiais com coeficientes em um corpo finito.

Informalmente, um corpo é um conjunto de elementos (números) fechado sobre as operações da adição, subtração, multiplicação e divisão por elementos não-nulos. Em outras palavras, um corpo, $C = \{A, +, .\}$, é formado por conjunto A munido de duas operações binárias, que denotaremos por + e ., tal que:
(i) Em relação à primeira operação (+).
(a) Vale a comutatividade;
(b) Vale a associatividade;
(c) Tem elemento neutro. Neste caso, como a operação é a adição usual, o elemento neutro "e" é o valor nulo, ou seja, $e = 0_A$;
(d) Tem elemento simétrico. Neste caso, como a operação é a adição usual, o elemento simétrico a' de um dado a em A é definido por: $a' = -a$.
(ii) Em relação à segunda operação (.).
(a') Valem a associatividade e a comutatividade;
(b') É distributiva em relação à primeira operação;
(c') Tem elemento neutro. Neste caso, como a operação é a multiplicação usual, o elemento neutro é o valor da unidade 1, ou seja, $e = 1_A$, e vale que $0 \neq 1$.
(d') Todo elemento diferente de zero tem elemento inverso. Neste caso, como a operação é a multiplicação usual, o elemento simétrico a' de um dado a em A é definido por: $a' = \frac{1}{a}$.

No final do século XVIII, Évarist Galois provou que para cada potência de primo q (isto é, $q = p^m$, com p primo e $m \geq 1$) existe um *corpo finito* com q elementos e todos estes são isomorfos, denotado por $GF(p^m)$. Assim, os corpos de Galois nada mais são do que corpos com um número finito de elementos.

O corpo finito mais simples tem dois únicos elementos, formado precisamente pelos elementos zero(0) e um (1). Para esclarecer como esses dois elementos formam um corpo, defina as seguintes tabelas para as operações de adição e multiplicação:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

As operações apresentadas nas tabelas são muito conhecidas. Na teoria dos números, elas representam os restos da divisão por 2, isto é, o $\mathbb{Z}_2$. Em termos lógicos, + e . representam, respectivamente, o "ou exclusivo" e a "conjunção", se considerarmos "0" como o valor falso e "1" como o valor verdadeiro.

A *característica* de um corpo é o menor número p tal que adicionando o número 1, p vezes, obtemos como resultado o valor 0. Todos os corpos finitos tem cardinal p^m, isto é, p^m elementos, para algum p primo (o qual é sua característica).

Se, em particular, $m = 1$ em $GF(p^m)$ então para cada primo p, o anel $\mathbb{Z}_p$ dos inteiros módulo p é um *corpo*. Isso porque, pelo teorema de Fermat, para cada inteiro a e para cada primo p, a não divisível por p, $a^{p-1} \equiv 1$ (mod p). Por exemplo, temos que:

- Para $p = 2$.
  - $a = 1 \Rightarrow 1^{2-1} = 1 \equiv 1$ (mod 2);
  - $a = 3 \Rightarrow 3^{2-1} = 3 \equiv 1$ (mod 2);
  - $a = 5 \Rightarrow 5^{2-1} = 5 \equiv 1$ (mod 2). E assim por diante.
- Para $p = 3$.
  - $a = 1 \Rightarrow 1^{3-1} = 1 \equiv 1$ (mod 3);
  - $a = 2 \Rightarrow 2^{3-1} = 2^2 = 4 \equiv 1$ (mod 3);
  - $a = 4 \Rightarrow 4^{3-1} = 4^2 = 16 \equiv 1$ (mod 3). E assim por diante.

Como para todo elemento $[a]$, $[a] \neq 0$, $a^{p-1} \equiv 1$ (mod p), logo todo $[a]$ de $\mathbb{Z}_p$ tem um inverso multiplicativo. Portanto, $\mathbb{Z}_p$ é um corpo.

Para $m > 1$, a cada primo p, associamos um polinômio irredutível $f(x)$ de grau m sobre $(\mathbb{Z}_p)$. Um polinômio $p(x)$ é dito *irredutível* se for impossível expressá-lo como um produto de dois polinômios, $a(x)b(x)$, de graus maiores ou iguais a 1.

Exitem diversas técnicas para achar tais polinômios irredutíveis, sendo uma delas o algoritmo descoberto por Berlekamp que encontra a fatoração de qualquer polinômio $g(x)$ em polinômios irredutíveis sobre $\mathbb{Z}_p[X]$. Por outro lado, também existem diversas tabelas de polinômios irredutíveis que podem ser usadas para fins práticos, como é o nosso caso. A tabela que apresentamos abaixo foi extraída de (Simon 1981), p. 143.

p	m	$f(x)$
2	2	$x^2 + x + 1$
2	3	$x^3 + x^2 + 1$
2	4	$x^4 + x^3 + 1$
2	5	$x^5 + x^3 + 1$
2	6	$x^6 + x^5 + 1$
2	7	$x^7 + x + 1$
3	2	$x^2 + x - 1$
3	3	$x^3 - x + 1$
3	4	$x^4 + x^3 - 1$
5	2	$x^2 + x + 2$
5	3	$x^3 + x^2 + 2$
7	2	$x^2 + x + 3$
11	2	$x^2 + x + 7$

Um polinômio irredutível $f(x)$ de grau m sobre $\mathbb{Z}_p$ é útil para a construção de $GF(p^m)$ se as potências $x^0, x^1, x^2, ..., x^{p^m-2}$ são, duas a duas, distintas módulo $f(x)$, pois assim o máximo

divisor comum entre cada potência e $f(x)$ será 1 (mdc$(x^i, f(x)) = 1$, para $i \in \{0, 1, ..., p^m - 2\}$) e, consequentemente, os elementos não nulos do anel quociente $\mathbb{Z}_p[x]/\langle f(x)\rangle$ terão inversos multiplicativos, ou seja, $\mathbb{Z}_p[x]/\langle f(x)\rangle$ é um corpo. Essas potências são os elementos do corpo $GF(p^m)$.

Exemplo 1.3.1. Consideremos o corpo de Galois $GF(4)$, com $p = 2$ e m = 2. Para encontrarmos os elementos desse corpo, tomamos o polinômio irredutível $x^2 + x + 1$ e calculamos os valores das potências de x, ou seja, $x^0, ..., x^{p^m-2}$. Logo,

k	**0**	**1**	**2**
$x^k(mod\ f)$	**1**	**x**	**x + 1**

Esses valores são obtidos por meio da relação de congruência em relação a f(x). Assim, $f(x) \equiv 0$ (mod f(x)). Diante disso:

$$x^0 = 1;$$
$$x^1 = x;$$
$$f(x) = x^2 + x + 1 = 0 \Rightarrow x^2 = -x - 1 =_{mod\ 2} x + 1.$$

Portanto, $GF(4) = \{0, 1, x, x + 1\}$

Seja F um anel comutativo qualquer, cuja *unidade* e *zero* são representados, respectivamente, por 1 e 0. Então $F[X]$ é o anel de todos os polinômios finitos nas variáveis $x_1, ..., x_n$, de grau arbitrário e cardinal p^m. Para o que nos interessa, tomemos F como um corpo finito, e portanto, como uma das estruturas $GF(p^m)$ (em particular, se m = 1, $\mathbb{Z}_p$).

Seja F um anel comutativo com unidade. Um **polinômio** (em uma coleção de variáveis x, $x \in X$) com coeficientes no anel F é uma expressão $p(x)$ da forma

$$p(x) = a_0 + a_1x^1 + ... + a_nx^n$$

em que $a_0, ..., a_n \in F$ e $n \in \mathbb{N}$.

Denotaremos por $F[X]$ o conjunto de polinômios sobre o anel F, ou seja:

$$F[X] = \{a_0 + a_1x + a_2x^2 + ... + a_nx^n / x \in X\}, a_i \in F, 0 \leq i \leq n,$$

Definição 1.3.2. (Adição de polinômios) Dados dois polinômios em $F[X]$,

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \text{ e } g(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m,$$

define-se

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + ... + (a_p + b_p)x^p,$$

onde p é o máximo de m e n, e $a_i = 0$ se $i > n$ e $b_i = 0$ se $i > m$.

Definição 1.3.3. (Multiplicação de polinômios) Dados dois polinômios em $F[X]$,

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \text{ e } g(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m,$$

define-se

$$f(x).g(x) = \sum_{k=0}^{m+n} c_k x^k = c_0 + ... + c_{n+m}x^{n+m},$$

sendo $c_k = \sum_{i+j=k} a_i b_j$, para cada k, $0 \leq k \leq m+n$

Definição 1.3.4. Definimos um (p,m)-Cálculo de Anel de Polinômio (**(p,m)-CAP**) para uma dada lógica $\mathcal{L}$, baseado no corpo de Galois $GF(p^m)$, onde p um número primo e m um número natural diferente de zero, como:

1. Todos os seus termos são variáveis e todas as suas fórmulas são polinômios de $GF(p^m)$;
2. As operações no **(p,m)-CAP** são manipuladas por um conjunto de regras básicas. São elas:
   a) Regras do Índice.
   Denotaremos por $\approxeq$ o operador de consequência do Cálculo de Anéis de Polinômios. Assim, temos:
   (a) $p \cdot x \approxeq 0$, onde $(p \cdot x)$ significa $(x + x + \ldots + x)$, sendo tal adição realizada p vezes.
   (b) $x^i \cdot x^j \approxeq x^k (mod\ q(x))$ em que $q(x)$ é um conveniente polinômio irredutível que define $GF(p^m)$, e $k = i + j (mod\ p^m - 1)$

   b) Regras de Anéis
   (a) $f + (g + h) \approxeq (f + g) + h$
   (b) $(f + g) \approxeq (g + f)$
   (c) $f + 0 \approxeq f$
   (d) $f + (-f) \approxeq 0$
   (e) $f \cdot (g \cdot h) \approxeq (f \cdot g) \cdot h$
   (f) $f \cdot (g + h) \approxeq (f \cdot g) + (f \cdot h)$

Há outras duas meta-regras dadas por:
Para $f, g, h \in F[X]$, temos:

1. Substituição Uniforme(SU) : $\frac{f \approxeq g}{f[x:h] \approxeq g[x:h]}$
2. Regra de Leibniz (RL): $\frac{f \approxeq g}{h[x:f] \approxeq h[x:g]}$

Sendo assim, o (p,m)-CAP para uma dada lógica $\mathcal{L}$ consiste basicamente em traduzir fórmulas de $\mathcal{L}$ em polinômios com coeficientes em um corpo finito, e realizar deduções através de operações sobre esses polinômios, sendo estas operações governadas pelo conjunto de regras básicas definidas acima.

Um dos problemas centrais deste trabalho é determinar qual (ou quais) são os melhores corpos finitos para servir de base à representação polinomial de uma dada lógica $\mathcal{L}$. Baseado nas ideias apresentadas em (Carnielli 2005b), as intuições subjacentes ao uso de polinômios ao invés de fórmulas para uma lógica finito valorada $\mathcal{L}$ podem ser vistas aqui.

Em resumo, definir um CAP para uma lógica específica consiste em:

1. Selecionar um corpo finito adequado, $GF(p^m)$, para representar os valores de verdade, escolhendo um subconjunto de elementos como valores designados.

2. Definir uma função de tradução de fórmulas em polinômios com coeficientes em $GF(p^m)$, ou seja,

$$* : For_{\mathcal{L}} \to GF(p^m)[X]$$

3. Em alguns casos, definir restrições polinomiais de tal modo que as operações sobre polinômios permitam realizar deduções válidas.

Para o caso do cálculo proposicional $\mathcal{L}$, um CAP é uma **tradução**, $* : \mathcal{L} \to \mathbb{Z}_2[X]$, de fórmulas de $\mathcal{L}$ em um conveniente anel de polinômio $\mathbb{Z}_2[X]$, com variáveis no conjunto X.

Para as definições de dedução e prova no cálculo dos anéis de polinômios para uma dada lógica $\mathcal{L}$, consideramos $\Gamma \cup \{\alpha\}$ fórmulas em $\mathcal{L}$ e Γ^* e α^* suas respectivas traduções. Assim,

$$\Gamma \vdash \alpha \text{ sse } \Gamma^* \mid\!\approx \alpha^*,$$

onde $\mid\!\approx$ denota a derivação de $\alpha^* \in D$ a partir de um conjunto de hipóteses $\Gamma^* \in D$ e D é o conjunto de valores de verdade distinguidos.

Quando o conjunto de distinguidos é unitário de 1, isto é, $D = \{1\}$, então a dedução $\Gamma^* \mid\!\approx \alpha^*$ se reduz a provar que $\alpha^* \approx 1$ a partir das hipóteses $\Gamma^* \approx 1$.

No entanto, quando fazemos as traduções das fórmulas de um dado sistema lógico em anéis de polinômios com coeficientes em um corpo finito, estamos apenas com a parte sintática do método.

A semântica associada consiste em interpretações $I : \mathbb{Z}_p[X] \to \mathbb{Z}_p$.

Observação 1.3.5. A álgebra de Lindenbaum-Tarski do cálculo proposicional clássico (CPC)

A ideia subjacente à algebrização de uma lógica está no desenvolvimento de uma álgebra a partir da assinatura da lógica em questão, de tal modo que esta álgebra expresse as propriedades da lógica.

De acordo com (Givant & Halmos 1974), a álgebra desenvolvida a partir da assinatura da lógica é conhecida como a *álgebra das fórmulas*, cujo universo é composto pelas fórmulas da lógica e suas operações são definidas a partir dos conectivos dessa lógica.

É importante salientarmos que a álgebra das fórmulas é uma álgebra livre na classe de todas as álgebras similares, no sentido em que gera irrestritamente todas as fórmulas a partir da assinatura e das variáveis proposicionais.

Em se tratando do CPC assumiremos, sintaticamente, que:

i) A assinatura do CPC é constituída por:

- Um conjunto enumerável de variáveis proposicionais:

$$X = \{x_0, ..., x_n, ...\}$$

- Conectivos proposicionais: $C = \{\neg, \rightarrow\}$;
- Símbolos metalinguísticos: parênteses, "$(,)$", e a vírgula, ",".

ii) Fórmulas.

O conjunto das fórmulas de $\mathcal{L}$, $For\{\mathcal{L}\}$, é formado pelas sequências de símbolos definidos acima, que satisfazem a seguinte definição recursiva:

1. Cada fórmula atômica, ou fórmulas atômicas, é uma fórmula;
2. Se φ é uma fórmula, então $(\neg\varphi)$ também é uma fórmula;
3. Se φ e ψ são fórmulas, então $(\varphi \rightarrow \psi)$ é uma fórmula;
4. As fórmulas são formadas apenas pelos ítens acima.

iii) Conjunto de Axiomas.

1. $\vdash_{CPC} \varphi \rightarrow (\psi \rightarrow \varphi)$
2. $\vdash_{CPC} (\varphi \rightarrow (\psi \rightarrow \lambda)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \lambda))$
3. $\vdash_{CPC} ((\neg\varphi \rightarrow \neg\psi) \rightarrow ((\neg\varphi \rightarrow \psi) \rightarrow \varphi))$.

iv) Regras.

- *Modus Ponens*: $\frac{\varphi, \varphi \rightarrow \psi}{\psi}$

Um sistema dedutivo S é uma estrutura da forma $\langle For, \vdash_S \rangle$, contendo um conjunto de fórmulas e uma relação de consequência.

Para algebrizar uma lógica, como por exemplo o CPC, devemos definir uma álgebra que separe menos as fórmulas e que permita desprezar, semanticamente falando, diferenças insignificantes entre as fórmulas, mas de tal modo que a composição resultante não esteja em desacordo com os conectivos. Para tanto, devemos aplicar o conjunto quociente nessa álgebra, por meio de uma relação de equivalência que seja também uma congruência.

Assim, sejam φ e ψ fórmulas de $For(\mathcal{L})$, definimos no CPC:

$$\varphi \cong \psi \text{ sse } [\varphi] = [\psi] \text{ see } \varphi \dashv\vdash \psi \text{ sse } \vdash_{CPC} \varphi \leftrightarrow \psi$$

Consequentemente, uma álgebra quociente pode ser definida de tal modo que seus elementos são classes de equivalência de fórmulas, e cujas operações são induzidas pelos conectivos da lógica. Assim, de acordo com Juliana Bueno em (Bueno-Soler 2004),

> "Este procedimento garante que cada classe de álgebra possa ser vista como a exata contraparte algébrica de sua lógica correspondente, no sentido em que existe uma correspondência muito próxima entre a teoria dedutiva da lógica e a teoria equacional da álgebra, entendendo-se por "equacional" a prática de se trabalhar com quase-identidades, isto é, com identidades condicionais e não apenas identidades."

Diante disso podemos demonstrar que a álgebra do CPC é a álgebra de Boole. Mais explicitamente, temos que a álgebra de Lindenbaum-Tarski associado ao CPC é isomorfa à álgebra de Boole livremente gerada por um conjunto infinito e enumerável. Os detalhes dessa demonstração estão em (Bueno-Soler 2004), p. 40.

Denotamos por $Lin\,(\mathcal{L})$ a álgebra de Boole livremente gerada pelo conjunto:

$$X = \{[x_k]\,, k \in \mathbb{N}\}\ ^{3}$$

De acordo com (Givant & Halmos 2009), p. 14, a teoria da álgebra booleana com os anéis booleanos estão intimamente relacionados. Na verdade, são apenas maneiras diferentes de olhar para o mesmo objeto.

Um *anel booleano* (BR: boolean ring) é um anel idempotente com unidade, isto é, é uma estrutura constituída por um universo, três operações, sendo duas binárias (adição e multiplicação) e uma unária (negação), e por dois elementos ditos distinguidos, 1 e 0, onde o inverso multiplicativo existe e tem valor 1 e, por fim, é válida a seguinte propriedade: $p.p = p$. Em resumo, $BR = \langle A, +, ., -, 0, 1\rangle$. O anel com 2 elementos, 0 e 1, é o mais simples exemplo de um anel booleano não-degenerativo, sendo representado pelo número 2 ou pelo conjunto $\{1, 0\}$.

A condição de idempotência na definição de um anel booleano exerce uma forte influência na estrutura desses anéis, tendo como consequência imediata que:

- um anel booleano sempre tem característica 2;
- Um anel booleano é sempre comutativo.

Seja X um conjunto arbitrário qualquer e $P(X)$ a classe de todos os subconjuntos de X. A classe $P(X)$, juntamente com as operações de união, intersecção, complementação, e pelos subconjuntos ditos distinguidos, o vazio ($\emptyset$) e o universo (X), é denominada *álgebra booleana* (BA: boolean algebra) de todos os subconjuntos de X. Isto é, $BA = \langle P(X), \cup, \cap, ', \emptyset, X\rangle$.

Apesar de haver importantes diferenças entre BR e BA, tal como o fato da distributividade da adição sobre a multiplicação falhar em BR, toda álgebra booleana pode ser transformada em anéis booleanos, e vice-versa, por meio de definições apropriadas das operações envolvidas no processo.

Para demonstrarmos que anéis booleanos podem ser definidos em termos de álgebra booleana, e vice-versa, compararemos a álgebra booleana $P(X)$ de todos os subconjuntos de X com o anel booleano 2^X de todas as funções bivaloradas em X.

Cada subconjunto P de X está naturalmente associado a uma função p de X em 2, isto é, está associado a sua função característica, definida em cada $x \in X$, por:

$$p(x) = \begin{cases} \mathbf{1}, & se\ \ x \in P \\ \mathbf{0}, & se\ \ x \notin P \end{cases} \tag{1.1}$$

A função que mapeia cada subconjunto para a sua função característica é uma bijeção de $P(x)$ em 2^X. A função inversa mapeia cada função q em 2^X para os conjuntos x em X para os quais $q(x) = 1$.

[3] $k \neq m \Rightarrow [x_k] \neq [x_m]$ pois $x_k \dashv\vdash x_m \Rightarrow k = m$

Parte 1: Como devem ser definidas as operações de adição e multiplicação, e os distinguidos 0 e 1 em $P(X)$ para que se tornem um anel Booleano?

Suponhamos que P e Q são subconjuntos de X e p e q suas funções características. Assim, temos:

$$p(x) = \begin{cases} \mathbf{1}, & se\ x \in P \\ \mathbf{0}, & se\ x \notin P \end{cases} \tag{1.2}$$

$$q(x) = \begin{cases} \mathbf{1}, & se\ x \in Q \\ \mathbf{0}, & se\ x \notin Q \end{cases} \tag{1.3}$$

A soma $(p+q)$ e o produto $(p.q)$ serão definidos ponto a ponto do seguinte modo: para todo x em X, temos:

$$p+q(x) = p(x) + q(x) = \begin{cases} \mathbf{1}, & se\ p(x) \neq q(x) \\ \mathbf{0}, & se\ p(x) = q(x) \end{cases} \tag{1.4}$$

Os valores $p(x)$ e $q(x)$ são diferentes apenas quando um deles é 1 e o outro é 0, isto é, apenas no caso em que $x \in P$ e $x \notin Q$, ou vice-versa. De modo análogo, os valores de $p(x)$ e $q(x)$ são ambos 1 apenas no caso em que x pertence a ambos, P e Q. A partir dessas observações concluímos que:

$$P + Q = (P \cap Q') \cup (P' \cap Q)$$

$$P.Q = P \cap Q$$

Uma análise similar sugere as seguintes definições:

$$0 = \emptyset$$

e

$$1 = X$$

para os elementos distinguidos do anel 0 e 1 em $P(X)$. Com estas operações e elementos distinguidos, o conjunto $P(X)$ torna-se um *anel booleano*.

Parte 2: Como devem ser definidas as operações de união e intersecção, e os distinguidos $\emptyset$ e X em 2^X para que este se torne uma álgebra booleana?

Suponhamos que P e Q são subconjuntos de X e p e q suas respectivas funções características. Então:
$x \in P \cup Q$ sse $x \in P$ ou $x \in Q$ (def. da união)

$x \in P \cup Q$ sse $p(x) = 1$ ou $q(x) = 1$ (função característica)

$x \in P \cup Q$ sse $p(x) \neq q(x)$ ou $p(x) = q(x) = 1$ $(2 = \{0, 1\})$

$x \in P \cup Q$ sse $p(x) + q(x) + p(x).q(x) = 1$

$x \in P \cup Q$ sse $(p + q + p.q)(x) = 1$

Do mesmo modo:

$x \in P'$ sse $x \notin P$

$x \in P'$ sse $p(x) \neq 1$

$x \in P'$ sse $p(x) \neq 1(x)$

$x \in P'$ sse $p(x) + 1(x) = 1$

$x \in P'$ sse $p + 1(x) = 1$

A partir dessas observações, podemos definir as operações de união e de coomplementar em 2^X do seguinte modo:

$$p \vee q = p + q + p.q$$
$$p' = p + 1$$

Uma análise similar que os elementos booleanos distinguidos $\emptyset$ e X coincidem com os elementos distinguidos do anel 0 e 1, bem como a intersecção coincide com a multiplicação. Com estas operações e elementos distinguidos, o conjunto 2^X torna-se uma álgebra booleana.

Tendo em vista essa observação, formalmente temos que:

Definição 1.3.6. Uma CAP-interpretação de formas polinomiais $\mathbb{Z}_p[X]$ em um corpo algébrico $\mathbb{Z}_p$ é um homomorfismo de anéis, que atribui a cada forma polinomial do CAP um valor no corpo finito $\mathbb{Z}_p$.

Em relação ao cálculo proposicional clássico, em que $\mathcal{L} = \{\neg, \wedge, \vee, \rightarrow\}$, uma função $v : For_{\mathcal{L}} \rightarrow \{0, 1\}$, tal que "1" representa o valor de verdade *verdadeiro* e "0" o valor de verdade *falso*, é uma **valoração** (clássica) se satisfaz as seguintes condições:

$$\begin{cases} v(\alpha \wedge \beta) = 1 \Rightarrow v(\alpha) = 1, v(\beta) = 1 \\ v(\alpha \wedge \beta) = 0 \Rightarrow v(\alpha) = 0 | v(\beta) = 0 \end{cases} \tag{1.5}$$

$$\begin{cases} v(\alpha \vee \beta) = 1 \Rightarrow v(\alpha) = 1 | v(\beta) = 1 \\ v(\alpha \vee \beta) = 0 \Rightarrow v(\alpha) = 0, v(\beta) = 0 \end{cases} \tag{1.6}$$

$$\begin{cases} v(\alpha \rightarrow \beta) = 1 \Rightarrow v(\alpha) = 0 | v(\beta) = 1 \\ v(\alpha \rightarrow \beta) = 0 \Rightarrow v(\alpha) = 1, v(\beta) = 0 \end{cases} \tag{1.7}$$

$$\begin{cases} v(\neg\alpha) = 1 \Rightarrow v(\alpha) = 0 \\ v(\neg\alpha) = 0 \Rightarrow v(\alpha) = 1 \end{cases} \tag{1.8}$$

Observação 1.3.7. A barra | denota a palavra "ou"

Em se tratando de polinômios, um CAP para a lógica proposicional clássica $\mathcal{L}$ é uma **tradução** de fórmulas de $\mathcal{L}$ em polinômios finitos com coeficientes no corpo $\mathbb{Z}_2$ e variáveis no conjunto (finito ou infinito) X, isto é, $* : For_{\mathcal{L}} \rightarrow \mathbb{Z}_2[X]$, tal que[4]:

[4]O processo de obtenção desses polinômios será visto na próxima seção.

1. $(p)^* = x_p$, para uma variável proposicional qualquer p. Quando não houver risco de confusão omitiremos o índice em x_p, escrevendo apenas x;

2. $(\alpha \wedge \beta)^* = \alpha^*.\beta^*$;

3. $(\alpha \vee \beta)^* = \alpha^*.\beta^* + \alpha^* + \beta^*$;

4. $(\alpha \rightarrow \beta)^* = \alpha^*.\beta^* + \alpha^* + 1$;

5. $(\neg\alpha)^* = \alpha^* + 1$;

A tradução $*$ define operações em polinômios correspondentes aos conectivos da linguagem $\mathcal{L}$, pois conforme vimos a cada álgebra de Boole associamos um anel de Boole.

Notemos que as traduções levam fórmulas em polinômios de grau n (finito e arbitrário) no anel $\mathbb{Z}_2[X]$, onde $X = \{x_p : p \in For_{\mathcal{L}}\}$. Diante disso, temos que os polinômios formam a sintaxe do método; a semântica associada consiste nas interpretações $I : \mathbb{Z}_2[X] \rightarrow \mathbb{Z}_2$.

As noções de tautologia, fórmulas válidas, etc..., em polinômios são definidos como no caso das fórmulas da linguagem proposicional, interpretando $1 \in \mathbb{Z}_2$ como *verdadeiro* e $0 \in \mathbb{Z}_2$ como o valor *falso*. Já a noção de prova é definida de forma distinta no método dos anéis de polinômios.

Definição 1.3.8. Um polinômio $p(x_1, ..., x_n) \in \mathbb{Z}_2[X]$ é um *teorema* do CPC se $p(x_1, ..., x_n) \approx 1$, por meio da aplicação das *regras básicas*.

Vamos mostrar que a tradução de formas proposicionais em polinômios é fiel, isto é, as operações no anel de polinômios correspondentes aos conectivos representam exatamente as condições semânticas para a lógica proposicional clássica (ou seja, reflete fielmente as valorações proposicionais).

Teorema 1.3.9. *Para cada valoração proposicional v, existe uma operação (tal como definida em $*$) e um homomorfismo de anéis $I : \mathbb{Z}_2[X] \rightarrow \mathbb{Z}_2$, tais que:*

$$v(\alpha) = I(\alpha^*), \textit{ isto é:}$$
$$v(\alpha) = 1 \textit{ sse } I(\alpha^*) = 1 \in \mathbb{Z}_2.$$

E, consequentemente:

$$v(\alpha) = 0 \textit{ sse } I(\alpha^*) = 0 \in \mathbb{Z}_2.$$

Demonstração: Seja $v : For_{\mathcal{L}} \rightarrow \{0, 1\}$ uma valoração. Definamos,
$I(x_p) = 1$ sse $v(p) = 1$;
$I(x_p) = 0$ sse $v(p) = 0$.

Em termos menos formais, temos:
$I(x_p) = v(p)$.

Só falta demonstrarmos que $v(\alpha) = I(\alpha^*), \alpha \in For$. Logo, por indução na complexidade das fórmulas, temos:

- Para a **negação**:
  $I(\neg\alpha)^* = 1 \Leftrightarrow I(\alpha)^* + 1 = 1 \Leftrightarrow_{\mathbb{Z}_2} I(\alpha)^* = 0 \Leftrightarrow_{HI} v(\alpha) = 0 \Leftrightarrow v(\neg\alpha) = 1.$

  $I(\neg\alpha)^* = 0 \Leftrightarrow I(\alpha)^* + 1 = 0 \Leftrightarrow_{\mathbb{Z}_2} I(\alpha)^* = 1 \Leftrightarrow_{HI} v(\alpha) = 1 \Leftrightarrow v(\neg\alpha) = 0.$

- Para a **conjunção**:
  $I(\alpha \wedge \beta)^* = I(\alpha)^*.I(\beta)^* = 1 \Leftrightarrow_{\mathbb{Z}_2} I(\alpha)^* = 1$ e $I(\beta)^* = 1 \Leftrightarrow_{HI} v(\alpha) = 1$ e $v(\beta) = 1 \Leftrightarrow v(\alpha \wedge \beta) = 1$.

  $I(\alpha \wedge \beta)^* = I(\alpha)^*.I(\beta)^* = 0 \Leftrightarrow_{\mathbb{Z}_2} I(\alpha)^* = 0$ ou $I(\beta)^* = 0 \Leftrightarrow_{HI} v(\alpha) = 0$ ou $v(\beta) = 0 \Leftrightarrow v(\alpha \wedge \beta) = 0$.

- Para $(\vee, \rightarrow)$ a demonstração é análoga.

■

O leitor terá notado que a demonstração acima, embora rigorosa, é um tanto quanto pedante. É conveniente simplificar a demonstração (alertando para o fato de que repetiremos muitas vezes este argumento) de forma a torná-la mais intuitiva. Nesses termos, a demonstração acima pode ser recolocada na seguinte maneira:

$$v(\alpha \wedge \beta) = 1 \Leftrightarrow \alpha^*.\beta^* = 1.$$

De fato, por um lado temos que:

$$v(\alpha \wedge \beta) = \begin{cases} \mathbf{1}, & sse\ v(\alpha) = 1, v(\beta) = 1 \\ \mathbf{0}, & c.c \end{cases} \tag{1.9}$$

Por outro lado,

$$\alpha^*.\beta^* = \begin{cases} \mathbf{1}, & sse\ \alpha^* = 1, \beta^* = 1 \\ \mathbf{0}, & c.c \end{cases} \tag{1.10}$$

Idem para os demais conectivos.

Sendo assim, uma fórmula $\alpha \in \mathcal{L}$ é **satisfatível** se sua tradução polinomial $\alpha^* \in \mathbb{Z}_2[X]$ é fechada dentro de um certo conjunto $\mathbf{D} \in F$ de valores distinguidos, quando valorado no corpo F. É conveniente, portando, mostrarmos que qualquer função finita pode ser expressa por meio de polinômios sobre corpos finitos usando para isto dois métodos distintos: *interpolação de Lagrange* e pela *resolução de sistemas lineares*. Exporemos cada um deles na próxima seção.

1.4 O processo de obtenção dos anéis de polinômios

1.4.1 Polinômios para sistemas verofuncionais.

O procedimento para a obtenção dos polinômios correspondente a uma lógica finito-valorada e determinística inicia-se com a construção das tabelas de verdade para cada um dos conectivos que compõem a linguagem do sistema lógico que será traduzido. Se, por exemplo, estivermos

trabalhando com o cálculo proposicional clássico (CPC), cuja linguagem é constituída por $\mathcal{L} = \{\wedge, \vee, \neg, \rightarrow\}$, temos as seguintes tabelas de verdade associadas a cada conectivo:

		$\wedge$
t	**t**	**t**
t	**f**	**f**
f	**t**	**f**
f	**f**	**f**

		$\vee$
t	**t**	**t**
t	**f**	**t**
f	**t**	**t**
f	**f**	**f**

		$\rightarrow$
t	**t**	**t**
t	**f**	**f**
f	**t**	**t**
f	**f**	**t**

	$\neg$
t	**f**
f	**t**

A partir deste ponto, para a caracterização dos polinômios correspondentes às fórmulas de um sistema lógico, temos a opção de prosseguir por meio de dois procedimentos distintos: por *interpolação de Lagrange* ou pela *resolução por sistemas lineares*. Apresentaremos, na íntegra, cada um deles a fim de tornar mais compreensíveis os cálculos dos próximos capítulos.

(i) **Resolução por Sistemas Lineares**

Como a própria nomenclatura sugere, a definição de uma lógica finito-valorada depende de um número finito n, $n \geq 2$, de valores de verdade. Sendo assim, se $n = 2$ tem-se um sistema com dois valores de verdade, ou seja, bivalorado; se $n = 3$, o sistema é dito trivalorado e assim por diante. Ao expressarmos estes valores de verdade em forma de matrizes, apresentamos todas as possíveis combinações que esses valores podem assumir mediante um dado conectivo lógico. E assim, a essa matriz podemos associar um polinômio na sua forma mais geral, o qual refletirá todas as propriedades das tabelas de verdade.

Seja, portanto, $\mathcal{L}$ uma lógica com n-valores de verdade e w um conectivo k-ário. Nesse contexto, a tabela de verdade de w tem n^k entradas e, portanto, o polinômio associado a esse conectivo deve ter k-variáveis distintas, com grau total menor ou igual a $k.(n-1)$ (pois temos n^k coeficientes para serem determinados).

Consideremos, como exemplo, um sistema com três valores de verdade, $n = 3$, com um conectivo binário, $k = 2$ e $X = \{x, y\}$. Neste caso, teremos uma matriz com 9 entradas, e o polinômio associado a esta matriz é explicitado por:

$$a_0 + a_1x + a_2y + a_3x^2 + a_4xy + a_5y^2 + a_6x^3 + a_7x^2y + a_8xy^2 + a_9y^3$$

Neste trabalho, restringir-nos-emos às tabelas de verdade unárias e binárias que representam a grande maioria dos conectivos lógicos nos sistemas finito-valorados.

Voltemos, portanto, às tabelas do CPC. Na linguagem definida acima temos um conectivo unário (a negação), três conectivos binários $(\vee, \wedge, \rightarrow)$ e o sistema é bivalorado. Podemos, então, associar polinômios n-ários gerais de grau 1, que representarão todas as possíveis tabelas de verdade em questão, ou seja:

$$p(x) = ax + b$$
$$p(x, y) = axy + bx + cy + d$$

Em um sistema trivalorado, cujos conectivos são do tipo unário e binário, temos os seguintes polinômios gerais unários e binários, respectivamente:

$$p(x) = ax^2 + bx + c$$
$$p(x,y) = ax^2y^2 + a'x^2y + a''x^2y^0 + bxy^2 + b'xy + b''xy^0 + cx^0y^2 + c'x^0y + c''x^0y^0$$

Generalizando, encontramos os seguintes polinômios em suas formas gerais:

- **Conectivos unários**

  1. Sistemas bivalorados: $p(x) = ax + b$.
  2. Sistemas trivalorados: $p(x) = ax^2 + bx + c$.
  3. Sistemas tetravalorados: $p(x) = ax^3 + bx^2 + cx + d$.
  4. Sistemas pentavalorados: $p(x) = ax^4 + bx^3 + cx^2 + dx + e$.
     $\vdots$
  5. Sistemas n-valorados: $p(x) = ax^{n-1} + bx^{n-2} + \cdots + kx^0$.

  Todos eles com coeficientes nos respectivos corpos finitos.

- **Conectivos Binários**

  1. Sistemas bivalorados: $p(x,y) = axy + bx + cy + d$.
  2. Sistemas trivalorados: $p(x,y) = ax^2y^2 + a'x^2y + a''x^2y^0 + bxy^2 + b'xy + b''xy^0 + cx^0y^2 + c''x^0y + c''x^0y^0$.
  3. Sistemas tetravalorados: $p(x,y) = ax^3y^3 + a'x^3y^2 + a''x^3y + a'''x^3y^0 + bx^2y^3 + b'x^2y^2 + b''x^2y + b'''x^2y^0 + cxy^3 + c'xy^2 + c''xy + c'''xy^0 + dx^0y^3 + d'x^0y^2 + d''x^0y + d'''x^0y^0$.
  4. Sistemas pentavalorados: $p(x,y) = ax^4y^4 + a'x^4y^3 + a''x^4y^2 + a'''x^4y + a''''x^4y^0 + bx^3y^4 + b'x^3y^3 + b''x^3y^2 + b'''x^3y + b''''x^3y^0 + cx^2y^4 + c'x^2y^3 + c''x^2y^2 + c'''x^2y + c''''x^2y^0 + dxy^4 + d'xy^3 + d''xy^2 + d'''xy + d''''xy^0 + ex^0y^4 + e'x^0y^3 + e''x^0y^2 + e'''x^0y + e''''x^0y^0$.
     $\vdots$
  5. Sistemas n-valorados: $p(x,y) = ax^{n-1}y^{n-1} + a'x^{n-1}y^{n-2} + \cdots + a^{(m)}x^{n-1}y^0 + bx^{n-2}y^{n-1} + b'x^{n-2}y^{n-2} + \cdots + b^{(m)}x^{n-2}y^0 + \cdots + kx^0y^{n-1} + k'x^0y^{n-2} + \cdots + k^{(m)}x^0y^0$.

Prosseguindo com o método para representar uma matriz em termos polinomiais, temos as seguintes etapas:
(a) A partir do tipo dos conectivos e da quantidade de valores de verdade do sistema a ser traduzido em anéis de polinômios, selecionamos os polinômios gerais associados a essas informações.
(b) A partir da matriz dos valores de verdade de cada conectivo, calculamos o valor de cada

entrada na matriz via polinômios.
(c) Após a substituição de todos os valores, teremos um sistema com um número finito de equações e incógnitas, o qual determina, após a sua resolução, o polinômio final associado àquele conectivo.

Como um exemplo, determinaremos os polinômios para o CPC seguindo os passos acima mencionados.
(a') Polinômios gerais: $p(x) = ax + b$ e $p(x, y) = axy + bx + cy + d$.
(b') Substituição dos valores de verdade.

- Para a conjunção.
  $p(0, 0) = 0 \Rightarrow a.0.0 + b.0 + c.0 + d = 0$. Portanto, $d = 0$.
  $p(1, 0) = 0 \Rightarrow a.1.0 + b.1 + c.0 + d = 0 \Rightarrow 0 + b + 0 + 0 = 0$. Portanto, $b = 0$.
  $p(0, 1) = 0 \Rightarrow a.0.1 + b.0 + c.1 + d = 0 \Rightarrow 0 + 0 + c + 0 = 0$. Portanto, $c = 0$.
  $p(1, 1) = 1 \Rightarrow a.1.1 + b.1 + c.1 + d = 1 \Rightarrow a + 0 + c + 0 = 1$. Portanto, $a = 1$.
  Neste caso, em virtude das várias ocorrência do valor 0, o sistema já está solucionado. Assim, o polinômio para a conjunção no CPC é dado por: $p_{\wedge}(x, y) = xy$.

- Para a disjunção.
  $p(0, 0) = 0 \Rightarrow a.0.0 + b.0 + c.0 + d = 0$. Portanto, $d = 0$.
  $p(1, 0) = 1 \Rightarrow a.1.0 + b.1 + c.0 + d = 1 \Rightarrow 0 + b + 0 + 0 = 1$. Portanto, $b = 1$.
  $p(0, 1) = 1 \Rightarrow a.0.1 + b.0 + c.1 + d = 1 \Rightarrow 0 + 0 + c + 0 = 1$. Portanto, $c = 1$.
  $p(1, 1) = 1 \Rightarrow a.1.1 + b.1 + c.1 + d = 1$.

  Neste momento temos o seguinte sistema: $a.1.1 + b.1 + c.1 + d = 1$;
  $d = 0$;
  $b = 1$;
  $c = 1$.
  Logo,
  $a + 1 + 1 + 0 = 1 \rightarrow a = 1$, pois como estamos em $\mathbb{Z}_2$ temos que $1 + 1 = 0$. Portanto, o polinômio para a disjunção no CPC é dado por: $p_{\vee}(x, y) = xy + x + y$.

- Para a implicação.
  $p(0, 0) = 1 \Rightarrow a.0.0 + b.0 + c.0 + d = 1$. Portanto, $d = 1$.
  $p(1, 0) = 0 \Rightarrow a.1.0 + b.1 + c.0 + d = 0 \Rightarrow 0 + b + 0 + 1 = 0$. Portanto, $b = 1$.
  $p(0, 1) = 1 \Rightarrow a.0.1 + b.0 + c.1 + d = 1 \Rightarrow 0 + 0 + c + 1 = 1$. Portanto, $c = 0$.
  $p(1, 1) = 1 \Rightarrow a.1.1 + b.1 + c.1 + d = 1 \Rightarrow a + 1 + 0 + 1 = 1$. Como estamos em $\mathbb{Z}_2$ temos que $1 + 1 = 0$. Portanto, $a = 1$.

  Logo, o polinômio para a implicação no CPC é dado por: $p_{\rightarrow}(x, y) = xy + x + 1$.

- Para a negação.
  $p(0) = 1 \Rightarrow a.0 + b = 1$. Portanto, $b = 1$.
  $p(1) = 0 \Rightarrow a.1 + b = 0 \Rightarrow a + 1 = 0$. Portanto, $a = 1$.
  Logo, o polinômio para a negação no CPC é dado por: $p_{\neg}(x) = x + 1$.

(c') Os respectivos polinômios são dados por:

$$p_{\neg}(x) = x + 1$$
$$p_{\wedge}(x, y) = xy$$
$$p_{\vee}(x, y) = xy + x + y$$
$$p_{\rightarrow}(x, y) = xy + x + 1$$

(ii) **Interpolação de Lagrange**

O objetivo subjacente ao desenvolvimento desses processos de obtenção de polinômios é a utilização de polinômios ao invés de fórmulas para sistemas lógicos finitamente multivalorados.

Walter Carnielli em (Carnielli 2007) demonstra que qualquer função finita pode ser expressa através de polinômios sobre corpos finitos, utilizando para isso um caso particular do método de Interpolação de Lagrange.

Teorema 1.4.1. *(Representação de funções finitas em um corpo de Galois): Seja A um conjunto qualquer finito com cardinalidade $|A| = k$, $f : A^m \to A$ uma função com m variáveis em A e $GF(p^n)$ o corpo de Galois com p^n elementos, sendo que $k \leq p$. Nestas condições, podemos representar f como uma função polinomial associada a um polinômio em $GF(p^n)[x_1, ..., x_m]$.*

Demonstração:

Esboçaremos a prova apenas para o caso de funções binárias. É claro que, de modo análogo ao que será realizado aqui, podemos obter o polinômio para o caso de uma função geral.

Suponhamos, sem perda de generalidade, que os elementos de A são $\{0, 1, ..., k-1\} \subset GF(p^n)$, com $k \leq p$. Definamos um polinômio $\delta_{\langle a,b\rangle}(x, y)$, com $\{a, b\} \in A$, como:

$$\delta_{\langle a,b\rangle}(x, y) = \prod_{\substack{i\neq a,\\ j\neq b,\\ i,j<k}} (x - i)(y - j) / \prod_{\substack{i\neq a,\\ j\neq b,\\ i,j<k}} (a - i)(b - j)$$

ou

$$\delta_{\langle a,b\rangle}(x, y) = \prod_{\substack{i\neq a,\\ j\neq b,\\ i,j<k}} \frac{(x - i)(y - j)}{(a - i)(b - j)}$$

Desta forma:

$$\delta_{\langle a,b\rangle}(a', b') = \begin{cases} \mathbf{1}, & se\ \ (a', b') = (a, b) \\ \mathbf{0}, & se\ \ (a', b') \neq (a, b) \end{cases} \tag{1.11}$$

Agora, se $f : A^m \to A$ tem valores $f(i, j) \in GF(p^n)$, então o polinômio que a representa será dado por:

$$p(x, y) = \sum_{a,b\in A}^{k^2} f(a, b).\delta_{\langle a,b\rangle}(x, y)$$

Isto é:

$$p(x, y) = f(0, 0).\delta_{\langle 0,0\rangle}(x, y) + f(0, 1).\delta_{\langle 0,1\rangle}(x, y) \ldots f(k-1, k-1).\delta_{\langle k-1,k-1\rangle}(x, y)$$

é um polinômio em $GF(p^n)(x_1, x_2)$, que representa $f(x, y)$. ∎

Exemplo 1.4.2. Novamente desenvolveremos os polinômios para o CPC, mas agora com o método de interpolação de Lagrange. Como funções de verdade para este sistema são binárias temos que:

$$p(x,y) = f(0,0).\delta_{\langle 0,0\rangle}(x,y) + f(0,1).\delta_{\langle 0,1\rangle}(x,y) + f(1,0).\delta_{\langle 1,0\rangle}(x,y) +$$

$$f(1,1).\delta_{\langle 1,1\rangle}(x,y)$$

Sendo assim:
$\delta_{\langle a,b\rangle}(x,y) = \prod_{\substack{i\neq a\\ j\neq b}} \frac{(x-i)(y-j)}{(a-i)(b-j)}$.

$\delta_{\langle 0,0\rangle}(x,y) = \frac{(x-1)(y-1)}{(-1)(-1)} = (x-1)(y-1)$.

$\delta_{\langle 0,1\rangle}(x,y) = \frac{(x-1)(y-0)}{(-1)(1)} = (x-1)(y)$.
Nota: $(-1) \equiv_2 1$. A congrurência ocorre em $\mathbb{Z}_2$ devido ao fato do sistema ser bivalente.

$\delta_{\langle 1,0\rangle}(x,y) = \frac{(x-0)(y-1)}{(1)(-1)} = (x)(y-1)$.

$\delta_{\langle 1,1\rangle}(x,y) = \frac{(x-0)(y-0)}{(1)(1)} = (x)(y)$.

Portanto:
$\delta_{\langle 0,0\rangle}(x,y) = (x-1)(y-1)$
$\delta_{\langle 0,1\rangle}(x,y) = (x-1)(y)$
$\delta_{\langle 1,0\rangle}(x,y) = (x)(y-1)$
$\delta_{\langle 1,1\rangle}(x,y) = (x)(y)$

Aplicando o método para o conectivo da conjunção, temos:
$f(0,0) = 0, f(0,1) = 0, f(1,0) = 0, f(1,1) = 0$
$p(x,y) = f(0,0)(x-1)(y-1) + f(0,1)(x-1)(y) + f(1,0)(x)(y-1) + f(1,1)(xy)$
$p(x,y) = 0.(x-1)(y-1) + 0.(x-1)(y) + 0.(x)(y-1) + 1(xy)$.
Portanto, $p_{\wedge}(x,y) = xy$.

Os demais conectivos são obtidos da mesma forma.

Para o caso da tradução de lógicas trivaloradas na forma polinomial, as funções $\delta_{\langle a,b\rangle}(x,y)$ são dadas por:
$\delta_{\langle 0,0\rangle}(x,y) = (x-1)(x-2)(y-1)(y-2)$.
$\delta_{\langle 0,1\rangle}(x,y) = (x-1)(x-2)(y)(y-2)$.
$\delta_{\langle 0,2\rangle}(x,y) = (x-1)(x-2)(y-1)(y)$.
$\delta_{\langle 1,0\rangle}(x,y) = (x)(x-2)(y-1)(y-2)$.
$\delta_{\langle 1,1\rangle}(x,y) = (x)(x-2)(y)(y-2)$.
$\delta_{\langle 1,2\rangle}(x,y) = (x)(x-2)(y)(y-1)$.
$\delta_{\langle 2,0\rangle}(x,y) = (x-1)(x)(y-1)(y-2)$.
$\delta_{\langle 2,1\rangle}(x,y) = (x-1)(x)(y)(y-2)$.
$\delta_{\langle 2,2\rangle}(x,y) = (x-1)(x)(y-1)(y)$.

Lembremos que, em $\mathbb{Z}_3$, $2 \equiv -1$ e, $4 \equiv 1$.

1.4.2 Polinômios para sistemas não-verofuncionais.

É notório que muitos sistemas lógicos, como a lógica intuicionista, as lógicas modais, várias lógicas paraconsistentes, não podem ser caracterizados por semânticas finito-valoradas.

Em (Carnielli 2005b), o autor propõe uma nova maneira de trabalhar polinomialmente com esses sistemas supracitados, através da inserção de um novo conjunto de variáveis X', disjunto do conjunto de variáveis já existente no sistema. Os elementos de X' serão denominados *termos ou variáveis ocultas*.

Variáveis ocultas são variáveis algébricas extras, distintas daquelas associadas às variáveis proposicionais, as quais tomam valor em um sistema de modo aleatório. Desta forma, sua aplicabilidade está intrinsecamente relacionada com sistemas que apresentam um certo inderterminismo, como é o caso do que ocorre na mecânica quântica. E isso explica o termo "oculto", usado em algumas interpretações da mecânica quântica.

A presença de variáveis ocultas no método de anel de polinômios, em sistemas lógicos não caracterizáveis matricialmente, desempenha um papel muito semelhante ao das variáveis ocultas da mecânica quântica: supõe-se que comportamentos inesperados possam ser explicados por variáveis presentes no sistema, mas sem controle epistêmico (isto é, desconhecidas, imprevisíveis, etc.). Diante disso, o valor de verdade de uma fórmula traduzida em um polinômio com variáveis ocultas não depende unicamente das variáveis proposicionais que compõem a fórmula, mas também das variáveis ocultas que aparecem na tradução.

O procedimento para obtenção dos polinômios com variáveis ocultas não é tão mecânico quanto aqueles para as lógicas caracterizáveis por matrizes finito-valoradas. No entanto, há uma certa heurística no método e buscaremos explicitar tal fato por meio de um sistema em particular, a Lógica da Inconsistência Formal mbC, que trataremos no capítulo 2.

1.5 Anéis de polinômios para o cálculo de primeira ordem monádico

Conforme discutimos nas seções anteriores, Ernst Schröder introduz dois novos símbolos com as seguintes características:
(i) O símbolo Σ é análogo à operação de disjunção na lógica.
(ii) O símbolo Π é análogo à operação de conjunção na lógica.

Sendo assim, para Schröder a quantificação poderia ser vista como um tipo de operação indefinida, na qual:
(a) Quantificação Universal ($\forall$): expressaria a multiplicação lógica indefinida.
(b) Quantificação Existencial ($\exists$): expressaria a adição lógica indefinida.

No entanto, em (Carnielli 2007), o autor apresenta uma abordagem distinta da de Schröder em relação a esta analogia entre operadores aritméticos e operadores lógicos. É importante salientarmos que, neste artigo, o autor define o cálculo de anéis de polinômios somente para a

parte **monádica** da lógica de primeira ordem (LPO) (os polinômios para a LPO serão discutidos no capítulo 5).

Definimos como LPO-monádica a um fragmento da lógica de primeira ordem no qual todos os símbolos de relações, definidos na assinatura do sistema, são do tipo monádicos, isto é, tem apenas um argumento ($P(x)$). Para a LPO-monádica, teremos uma função, $*$, que traduzirá fórmulas da LPO-monádica em polinômios sobre o corpo finito $\mathbb{Z}_2$. Assim, temos que $* : For_{FOL} \to \mathbb{Z}_2[X]$, onde todas as regras dos polinômios para o cálculo proposicional clássico são válidas, onde $A(x)$ representa um predicado unário e, além disso:

1. $(A(c_i))^* = x_i^A$, para cada constante c_i de um universo enumerável.
2. $(\forall x A(x))^* = \prod_{i=1}^{\infty} x_i^A$.
3. $(\exists x A(x))^* = (\neg\forall x \neg A(x))^* = 1 + \prod_{i=1}^{\infty}(1 + x_i^A)$

Notemos que, os "polinômios" agora são "séries formais" em $\mathbb{Z}_2[X]$, isto é, os polinômios são infinitos. Diante disso, para simplificarmos a notação usaremos:
1.$(\forall x A(x))^* = \prod x_i$.
2.$(\exists x A(x))^* = 1 + \prod(1 + x_i)$

Definição 1.5.1. Seja F um anel booleano, X um conjunto de variáveis algébricas e $*$ a função tradução de fórmulas do fragmento monádico da lógica de primeira ordem $\mathcal{L}$ a polinômios em F[X]. Considerando $D \subset F(D \neq \emptyset)$ como sendo o conjunto de valores distinguidos. Uma fórmula α de $\mathcal{L}$ é uma $\mathcal{L}$-CAP-conseqüência do conjunto de fórmulas Γ de $\mathcal{L}$ (o que será denotado por $\Gamma \mid\!\approx_{\mathcal{L}} \alpha$) se, para toda L-CAP-interpretação v, tem-se que $\alpha^*[\vec{X}_v] \in D$ sempre que $\gamma^*[\vec{X}_v] \in D$ para toda fórmula $\gamma \in \Gamma$.

Notação 1.5.2. A atribuição de valores às variáveis em X dada por uma valoração (ou interpretação) v será denotada $\vec{X}_v$, e o valor do polinômio P para a valoração v será denotada por $P[\vec{X}_v]$.

Nos casos em que D é um conjunto unitário ($D = \{d\}$) temos que $\mid\!\approx_{\mathcal{L}} \alpha$ se e somente se α^* é redutível, através das regras do CAP para $\mathcal{L}$, ao polinômio constante d.

Observação 1.5.3. Como $\mid\!\approx_{\mathcal{L}} \alpha$, conforme exposto acima, denota que α é uma consequência do cálculo de anéis de polinômios, usaremos o símbolo $\approx$ para a redução da fórmula em uma versão polinômica, bem como, na aplicação de uma regra do CAP com o intuito de reduzir o polinômio ao valor distinguido ou ao conjunto dos valores ditos distinguidos.

O seguinte exemplo mostra como são realizadas as deduções no CAP para o fragmento monádico da lógica de primeira ordem.

Exemplo 1.5.4. $\mid\!\approx_{\mathcal{L}} \forall x A(x) \to \exists x A(x)$.

$(\forall x A(x) \to \exists x A(x))^* \approx (\forall x A(x))^*(\exists x A(x))^* + (\forall x A(x))^* + 1 \approx$

$\approx (\prod x_i) \cdot (1 + \prod(1 + x_i)) + \prod x_i + 1$

$\approx_{distrib.} (\prod x_i) + (\prod x_i).(\prod(1 + x_i)) + \prod x_i + 1$

$\approx_{assoc.generalizada} (\prod x_i) + (\prod x_i.(1 + x_i)) + \prod x_i + 1$

$\approx (\prod x_i) + (\prod 0) + \prod x_i + 1$

$\approx \prod x_i + \prod x_i + 1$

$\approx 0 + 1$

≈ 1

já que $\prod x_i + \prod x_i = 0$ e $x_i \cdot (1 + x_i) = x_i + x_i = 0$ para cada x_i.

Portanto, $(\forall z A(z) \to \exists z A(z))^* \approx 1$.

Note que a computação acima utiliza uma versão da lei do índice aplicada a objetos infinitários, isto é, S(x) é um polinômio infinito e estamos supondo que:

$$S(x) + S(x) = 0$$
e
$$S(x).S(x) = S(x).$$

Observação 1.5.5. Demonstrar a consistência de tais operações infinitárias era um problema em aberto, o qual está relacionado com o material do capítulo 5.

O método de polinômios, assim como o método de provas por Tableaux, pode também ser usado para encontrarmos contra-exemplos, o que veremos agora.

Exemplo 1.5.6. $(\forall x A(x) \to \forall x B(x)) \to \forall x(A(x) \to B(x))$.
Sejam:
$\alpha = (\forall x A(x) \to \forall x B(x))$.
$\beta = \forall x(A(x) \to B(x))$.
$(\alpha \to \beta)^* \approx \alpha^*\beta^* + \alpha^* + 1$.
Então:
$(\alpha)^* \approx (\forall x A(x) \to \forall x B(x))^* \approx (\forall x A(x))^*(\forall x B(x))^* + (\forall x A(x))^* + 1 \approx$
$\approx \prod x \prod y + \prod x + 1 =_{assoc.generalizada} \prod(xy) + \prod x + 1$. Então, $(\alpha)^* \approx \prod(xy) + \prod x + 1$.
$(\beta)^* \approx (\forall x(A(x) \to B(x)))^* \approx \prod(xy + x + 1)$. Portanto, $(\beta)^* \approx \prod(xy + x + 1)$.

$(\alpha \to \beta)^* \approx (\prod(xy) + \prod x + 1)(\prod(xy + x + 1)) + (\prod(xy) + \prod x + 1) + 1 \approx$

$\approx \prod xy(xy + x + 1) + \prod x(xy + x + 1) + \prod(xy + x + 1) + \prod xy + \prod x + 1 + 1$

$$\approx \prod xy + \prod xy + \prod xy + \prod xy + \prod x + \prod x + \prod(xy + x + 1) + \prod xy + \prod x$$

$$\approx \prod(xy + x + 1) + \prod xy + \prod x \neq 1.$$

Para mais exemplos e aplicações do método de polinômios para lógicas finito-valoradas ver (Carnielli 2010), (Carnielli 2007) e (Carnielli 2005b).

1.6 As potencialidades do método de provas por anéis de polinômios

Qualquer pessoa, com um conhecimento mínimo em matemática, conhece e realiza operações com polinômios. Os polinômios, por serem simples e necessitarem de conceitos básicos de aritmética para a sua compreensão, podem ser vistos como uma ferramenta poderosa de provador automático de teoremas em lógica clássica e não-clássica.

Além disso, conforme discutiremos nesta tese, o método de anel de polinômios pode ser utilizado em sistemas lógicos não-verofuncionais, como as lógicas paraconsistentes, nos sistemas não-determinísticos de Arnon Avron e nos sistemas bivalentes que sofreram redução nos moldes da chamada Redução de Suszko.

Temos, portanto, uma ferramenta algébrica capaz de ser manipulada com facilidade pelos dispositivos computacionais, onde uma infinidade de lógicas não-clássicas, além da própria clássica, pode ser especificada. Além disso, o método pode ser usado para comparar sistemas lógicos.

Uma característica interessante do método é que não comparamos apenas distintos sistemas lógicos apresentados em suas versões polinomiais, mas também, comparamos o mesmo sistema quando este se apresenta na sua semântica tradicional n-valorada, ou então, com suas apresentação reduzida a uma semântica bivalorada segundo a redução de Suszko.

Analisaremos o caso particular da lógica paraconsistente trivalente de Sette, P_3^1. Para este sistema, temos um conjunto de polinômios resultante no corpo $\mathbb{Z}_3$ ou anel $\mathbb{Z}_3[X]$, referente à lógica verofuncional trivalente P_3^1, dado por:

$$(\neg\alpha)^* = 2x^2 + x + 2;$$
$$(\alpha \Rightarrow \beta)^* = 2x^2y^2 + x^2 + 2$$

E também temos um outro polinômio obtido em $\mathbb{Z}_2[X \cup X']$, onde X' é um conjunto de variáveis ocultas, resultante da tradução de fórmulas do sistema bivalorado reduzido de P_3^1. Os polinômios em questão são:

$$(\neg\alpha)^* = \alpha^* \cdot x_\alpha + 1, \text{ onde } x_\alpha \text{ é uma variável oculta.}$$
$$(\neg\neg\alpha)^* = (\alpha^* \cdot x_\alpha + 1) \cdot x_\alpha + 1.$$

Podemos observar que estes polinômios apresentam naturezas completamente diferentes, sendo, portanto, dois grupos de polinômios distintos para o mesmo sistema.

E de fato, os polinômios para P_3^1 em sua versão trivalorada e os polinômios para a sua versão bivalorada devem ser distintos, já que os sistemas apresentam características divergentes quanto

a questão da verofuncionalidade. A presença das variáveis ocultas vêm ao encontro da questão da perda da verofuncionalidade dos sistemas reduzidos pela redução de Suszko.

A implementação do método de prova por anéis de polinômios é efetivamente simples, já que se trata de um mecanismo que possui em sua composição e desenvolvimento apenas polinômios. Apesar de, na maioria das vezes, a tradução de fórmulas mais complexas em um formato polinomial, ser manualmente complicada, a utilização de dispositivos computacionais torna essa operação rápida e de fácil resolução, nos casos mais simples.

Como existem diversos métodos de provas para diferentes sistemas lógicos, também há distintas álgebras associadas a essas lógicas, tais como, a Álgebra Booleana associada a lógica proposicional clássica, a Álgebra de Heyting para as lógicas intuicionistas, a Álgebra Cilíndrica para a Lógica de Primeira Ordem, etc. No entanto, algebrizar lógicas multivalentes e modais é uma tarefa um pouco mais complicada e a algebrização da lógica paraconsistente apresenta um desafio real. Em (Agudelo & Carnielli 2011), os autores apresentam uma estreita relação entre o cálculo de polinômios e as lógicas modais.

Poderíamos pensar em utilizar os anéis de polinômios como um novo sistema algébrico, o qual algebrizaria os mais diversos sistemas lógicos de um modo mais natural e intuitivo. Essa "nova algebrização" poderia, então, resgatar a tradução quase natural do sistema lógico para o algébrico, um tanto quanto perdido com as formalizações algébricas contemporâneas propostas na literatura, especialmente para lógicas multivalentes e paraconsistentes.[5]

E, por fim, o método de polinômios pode ser visto como um dispositivo heurístico no sentido de descobrir novos sistemas lógicos ou novas propriedades de sistemas lógicos, conforme exposto em (Carnielli 2010), onde o autor define "Half-logics e quarter-logics", baseadas em conectivos não verofuncionais desenvolvidos por Jean-Yves Béziau. Em suma, demonstra-se que novas lógicas podem ser descobertas utilizando os polinômios como uma ferramenta heurística.

Fica claro, portanto, que o cálculo de anel de polinômios tem amplas potencialidade como mecanismo de automação pois constitui um dos poucos mecanismos para a exploração do lado heurístico da lógica, pode ser usado nos mais distintos sistemas não-clássicos e ainda introduz mecanismos que ajudam a entender e explicar certas características inerentes aos sistemas aos quais eles estão sendo aplicados. Assim, este método ajuda a tornar as provas lógicas mais interessantes e eficientes, comparável ao método dos tableaux.

[5]No entanto, deve-se notar que uma proposta heterodoxa de se algebrizar lógicas paraconsistentes é proposta por Juliana Bueno-Soler e Walter Carnielli em "*Possible-translations algebraization for paraconsistent logics", em Bulletin of the Section of Logic*", v. 34, n.2, p. 77-92, 2005.

Capítulo 2

Uma abordagem polinomial para as Lógicas Paraconsistentes na versão das LFIs

> "Logic is the study of reasoning; and mathematical logic is the study of the type of reasoning done by mathematicians. To discover the proper approach to mathematical logic, we must therefore examine the methods of the mathematician".
> (Joseph R. Shoenfield in *Mathematical Logic*, p. 1).

As Lógicas da Inconsistência Formal - LFIs- constituem uma classe de lógicas paraconsistentes cuja principal característica é a sua capacidade de recapturar o raciocínio consistente por meio do acréscimo de apropriadas proposições de consistência. Neste capítulo definimos uma boa parte das LFIs em uma versão polinômica, sendo de nossa inteira responsabilidade as definições referentes às lógicas bC, Ci, mbCe, mCie, bCe, Cie e LFI1 e as demonstrações dos seguintes teoremas: 2.3.14, 2.3.15, 2.3.16, 2.4.5, 2.5.6, 2.5.8 e 2.5.10. Além disso, melhoramos as apresentações polinomiais para os sistemas mbC e mCi, que foram detalhadamente redefinidas.

2.1 As Lógicas da Inconsistência Formal - LFIs.

Se desejamos entender a natureza e o significado da lógica devemos considerar que, atualmente, a lógica é um campo de conhecimento de mesma natureza da matemática.

Em um artigo de 1912 intitulado "*Imaginary (non-Aristotelian) logic*", Nikolay Vasiliev (1880- 1940) defende a possibilidade da construção de uma lógica não-aristotélica, cujo princípio norteador era o seguinte, conforme (Fonte 1983): assim como a geometria, a lógica pode ser apresentada como um sistema axiomático e, portanto, seria perfeitamente racional imaginar que a eliminação de alguns desses axiomas não afetaria o caráter lógico do sistema obtido, assim como ocorreu com a negação do quinto postulado de Euclides.

De acordo com (Arruda 1990), a lógica não-aristotélica proposta por Vasiliev é caracterizada pela substituição da Lei do Terceiro Excluído pela do Quarto-Excluído, e o *Princípio da Contradição* na forma "A não pode ser ao mesmo tempo, e sob o mesmo aspecto, B e não B", não é válido. Na realidade, em se tratando da contradição, o foco de Vasiliev não era abordar o problema da existência, ou não, de contradições no mundo real, mas sim em um mundo cujas

características determinam operações lógicas diferentes daquelas que ocorrem na interação com os objetos reais.

Diante disso, a lógica de Vasiliev tem como objeto um *mundo ideal*, criado pela imaginação e por isso é denominada por *Lógica Imaginária*. E, à medida que esse mundo imaginário se torna complexo, a lógica também transforma-se em mais complexa, podendo assim culminar com um sistema que pode ter mais de duas dimensões, no sentido de um número qualquer de qualidades do predicado. Nesse contexto, Vasiliev apresenta uma generalização para a sua lógica, obtendo lógicas de quaisquer dimensões, isto é, um sistema com um número qualquer de qualidades do predicado.

Na construção de sua lógica Vasiliev não usou notações lógicas, muito menos o formalismo emergente da lógica matemática. No entanto, o espírito da sua lógica imaginária foi estritamente não-aristotélica. Essas ideias de Vasiliev foram quase que completamente negligenciadas por quase meio século, mas mesmo assim, ele deu partida na emergência das lógicas não-clássicas.

Em 1910, Łukasiewicz aborda a possibilidade da existência de lógicas sem o Princípio da Contradição. No entanto, o primeiro sistema formal construído a partir da eliminação de certos princípios lógicos só aparece em 1948 com os trabalhos do polonês S. Jaskowski (1906-1965), discípulo de Łukasiewicz.

Jaskowski apresenta um calculo proposicional que conserva a validade do Princípio da Contradição, $\neg(A \wedge \neg A)$, mas elimina o Princípio do Terceiro Excluído. Tal lógica ficou conhecida como *Lógica Discussiva* ou *Lógica Discursiva*.

Concomitantemente e independentemente, o lógico brasileiro Newton C. A. da Costa também desenvolveu sistemas lógicos que envolviam contradições, mas diferentemente de Jaskowski que ficou apenas no âmbito proposicional, os trabalhos de Newton da Costa também abrangeram o cálculo de predicados com e sem a igualdade, cálculo com descrições, teoria de conjuntos. Por isso, Newton da Costa é reconhecido internacionalmente como o criador das lógicas paraconsistentes.

A paraconsistência é o estudo de teorias contraditórias que ainda não são triviais, ou seja, podemos ter contradições nessas teorias. No entanto, se o sistema da teoria em questão for consistente, então consistência e contradição geram trivialidade. Em resumo,

$$\text{Contradição} + \text{Consistência} = \text{Trivialidade}$$

Dito de modo não muito rigoroso, uma lógica é paraconsistente se ela pode fundamentar sistemas que admitam teses contraditórias mas que não sejam triviais, no sentido de que nem todas as fórmulas sejam teoremas do sistema. É importante salientarmos que a essência da lógica paraconsistente reside no *Princípio da Explosão*, ao invés da *Não-Contradição*, e tal fato será analisado em maiores detalhes neste capítulo, assim como a distinção existente entre esses princípios e o *Princípio da Não-Trivialidade*.

Quando Newton da Costa propôs sua primeira lógica paraconsistente, a ideia subjacente era que a *consistência* de uma dada fórmula não seria apenas um requisito para garantir o seu caráter não explosivo, mas também que tal conceito poderia ser representado por uma fórmula ordinária da linguagem padrão, tal como por exemplo, $(\alpha \wedge \neg\alpha)$.

Nossa intenção neste capítulo é traduzir em uma versão polinômica o conjunto de lógicas paraconsistentes, denominadas *Lógicas da Inconsistência Formal* (**LFI**), as quais internalizam

as noções de consistência e inconsistência dentro da sua linguagem objeto por meio da introdução de novos operadores no escopo da sua linguagem, permitindo-nos assim separar as noções de contradição e inconsistência.

No entanto, para prosseguirmos com o nosso trabalho, algumas definições de consistência, inconsistência, variedades de explosão e trivialidade precisam ser ilustrados, o que o faremos na próxima subseção. Essas definições foram extraídas de (Carnielli et al. 2007).

2.2 Conceitos e definições

Assumiremos que toda linguagem $\mathcal{L}$ será definida sobre a assinatura proposicional $\Sigma = \{\Sigma_n\}_{n\in\omega}$ tal que Σ_n é o conjunto de conectivos de aridade n. Seja $P = \{p_n : n \in \omega\}$ o conjunto de variáveis proposicionais (ou fórmulas atômicas) a partir do qual se gera a álgebra de fórmulas *For* através de Σ.

Informalmente, denominamos por *álgebra* uma estrutura composta por um domínio (ou universo de discurso) munida de um conjunto de operações. A *álgebra das fórmulas*, *For*, é uma álgebra desenvolvida a partir da assinatura da lógica, sendo portanto seu universo composto por fórmulas da lógica e suas operações definidas a partir dos conectivos da lógica.

Dado um conjunto X, $\wp(X)$ é definido como o conjunto das partes de X. Seja *For* um conjunto de fórmulas e $\vdash$ uma relação entre um conjunto Γ de fórmulas e uma fórmula φ, tal que $\vdash \subseteq \wp(For) \times For$. Quando a relação $\vdash$ satisfaz algumas das cláusulas abaixo, a classificamos como um operador de fecho ou como uma relação de consequência. Assim, para todas as fórmulas α e β, e subconjuntos Γ e Δ de *For*, temos:

(Con1): $\alpha \in \Gamma$ implica $\Gamma \vdash \alpha$. (Reflexividade)

(Con2):($\Delta \vdash \alpha$ e $\Delta \subseteq \Gamma$) implica $\Gamma \vdash \alpha$. (Monotonicidade)

(Con3): $(\forall \beta \in \Delta)$ $(\Gamma \vdash \beta$ e $\Delta \vdash \varphi) \Rightarrow \Gamma \vdash \alpha$ (corte)

(Con4): $\Gamma \vdash \alpha$ implica $\Gamma'_{fin} \vdash \alpha$ para algum $\Gamma'_{fin} \subseteq \Gamma$ (Finitariedade)[1]

(Con5): $\Gamma \vdash \alpha$ implica $\sigma(\Gamma) \vdash \sigma(\alpha)$, para toda substituição σ. (Estruturalidade)

Em termos sintáticos, estruturalidade corresponde à regra da substituição uniforme ou ao uso de esquemas de axiomas ou regras.

Se $\vdash$ satisfaz as cláusulas (Con1)-(Con3), $\vdash$ induz um *operador de fecho*. Se o operador de fecho satifizer as cláusulas (Con4) e (Con5) então ele é classificado como uma *relação de consequência tarskiana*.

Uma lógica **L** é definida como uma estrutura da forma $\langle For, \vdash \rangle$, contendo um conjunto de fórmulas e a relação de consequência definida acima. Por conveniência, suporemos que *For*

[1] A notação Γ'_{fin} indica que Γ é um conjunto finito.

é construído a partir de uma linguagem enumerável e que tem como conectivo primitivo a $\neg$ (negação). Qualquer conjunto $\Gamma \subseteq For$ é uma *teoria* **L**.

Definição 2.2.1. Seja Γ uma teoria de **L**. Dizemos que Γ é *contraditória* com relação a $\neg$, ou apenas contraditória, se ela satisfaz a seguinte condição:

$$\text{Existe } \alpha \text{ tal que, } (\Gamma \vdash \alpha \text{ e } \Gamma \vdash \neg\alpha)$$

Definição 2.2.2. Uma teoria Γ é dita ser *trivial* se e somente se:

$$\forall\alpha\,(\Gamma \vdash \alpha)$$

Sendo assim, dizemos que uma lógica **L** é *contraditória* se todas as suas teorias são contraditórias, isto é:

$$\forall\Gamma\exists\alpha(\Gamma \vdash \alpha \text{ e } \Gamma \vdash \neg\alpha)$$

Definição 2.2.3. Uma teoria Γ é dita ser *explosiva* se e somente se:

$$\forall\alpha\forall\beta\,(\Gamma, \alpha, \neg\alpha \vdash \beta)$$

Do mesmo modo, podemos afirmar que uma lógica **L** é *trivial* se todas as suas teorias são triviais e **L** é *explosiva* se todas as suas teorias são explosivas.

Com essas definições podemos agora apresentar uma definição formal de alguns *princípios lógicos* fundamentais para uma dada lógica **L**.

i) Princípio da Não-Contradição:

$$\exists\Gamma\forall\alpha(\Gamma \nvdash \alpha \text{ ou } \Gamma \nvdash \neg\alpha) \text{ (}\mathbf{L}\text{ é não-contraditória)} \quad (1)$$

ii) Princípio da Não-Trivialidade:

$$\exists\Gamma\exists\alpha(\Gamma \nvdash \alpha) \text{ (}\mathbf{L}\text{ é não-trivial)} \quad (2)$$

iii) Princípio da Explosão ou Pseudo-Scotus:

$$\forall\Gamma\forall\alpha\forall\beta(\Gamma, \alpha, \neg\alpha \vdash \beta) \text{ (}\mathbf{L}\text{ é explosiva)} \quad (3)$$

Para a definição das LFIs precisaremos de um conceito moderado a respeito da explosão, o que denominaremos por *gentilmente explosivo* ou *moderadamente explosivo*. É evidente, a partir do que foi exposto, que as Lógicas Paraconsistentes são instrumentos a serem utilizados em raciocínios que não pressupõem a consistência. E se entendemos a consistência como algo que pode faltar a uma contradição para tornar esse sistema explosivo, então claramente podemos expressar a consistência de uma fórmula no nível linguagem-objeto. E será este recurso que mais adiante nos permitirá recuperar o raciocínio consistente dentro de um ambiente inconsistente. Em termos formais temos:

Definição 2.2.4. Consideremos um conjunto de fórmulas $\bigcirc(p)$, possivelmente vazio, que depende apenas da variável proposicional p, e que satisfaça o seguinte:

(i) $\bigcirc\alpha, \alpha \nvdash \beta$
(ii) $\bigcirc\alpha, \neg\alpha \nvdash \beta$

Uma teoria Γ é dita *gentilmente explosiva*, com relação a $\bigcirc(p)$, se:

$$\forall\alpha\forall\beta(\Gamma, \bigcirc\alpha, \alpha, \neg\alpha \vdash \beta).$$

Uma teoria Γ gentilmente explosiva é *finita* apenas quando $\bigcirc(p)$ é um conjunto finito. Uma lógica $\mathcal{L}$ será dita (finitamente) gentilmente explosiva quando há um conjunto (finito) $\bigcirc(p)$ tal que todas as teorias de $\mathcal{L}$ são (finitamente) gentilmente explosiva (com relação a $\bigcirc(p)$).

Para qualquer fórmula α, o conjunto $\bigcirc(\alpha)$ expressará, em um sentido específico, a consistência de α para a lógica $\mathcal{L}$. Quando este conjunto é unitário, denotamos por $\circ\alpha$ o único elemento de $\bigcirc(\alpha)$ e, neste caso, $\circ$ define o *conectivo de consistência*.

Podemos, a partir da definição acima, considerar outras duas versões do Princípio da Explosão. São elas:
Princípio da Explosão Moderada: **L** é gentilmente explosiva em relação a algum conjunto $\bigcirc\alpha$.
Princípio da Explosão Moderada Finita: **L** é gentilmente explosiva em relação a algum conjunto *finito* $\bigcirc\alpha$.

Definição 2.2.5. Uma Lógica da Inconsistência Formal, **LFI**, é qualquer sistema lógico em que o Princípio da Explosão Moderada ocorre, em detrimento ao Princípio da Explosão.

2.3 Uma fundamental LFI: a lógica mbC.

Seja Σ° a assinatura constituída por $\Sigma^\circ = \{\wedge, \vee, \rightarrow, \neg, \circ\}$ tal que $\mathcal{P} = \{p_n : n \in \omega\}$ é o conjunto de fórmulas atômicas e $\circ$ um operador unário. Definiremos For° como o conjunto de fórmulas livremente geradas por $\mathcal{P}$ sobre For° .

Definição 2.3.1. Seja Σ° a assinatura composta por $\Sigma^\circ = \{\wedge, \vee, \rightarrow, \neg, \circ\}$. A lógica **mbC**, $mbC = \langle For^\circ, \vdash_{mbC}\rangle$, é formalizada pelo seguinte esquema de axiomas:
(Ax1) $\alpha \rightarrow (\beta \rightarrow \alpha)$
(Ax2) $(\alpha \rightarrow \beta) \rightarrow ((\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \gamma))$
(Ax3) $\alpha \rightarrow (\beta \rightarrow (\alpha \wedge \beta)$
(Ax4) $(\alpha \wedge \beta) \rightarrow \alpha$
(Ax5) $(\alpha \wedge \beta) \rightarrow \beta$
(Ax6) $\alpha \rightarrow (\alpha \vee \beta)$
(Ax7) $\beta \rightarrow (\alpha \vee \beta)$
(Ax8) $(\alpha \rightarrow \gamma) \rightarrow ((\beta \rightarrow \gamma) \rightarrow ((\alpha \vee \beta) \rightarrow \gamma))$
(Ax9) $\alpha \vee (\alpha \rightarrow \beta)$
(Ax10) $\alpha \vee \neg\alpha$
(bc1) $\circ\alpha \rightarrow (\alpha \rightarrow (\neg\alpha \rightarrow \beta))$.

Regra de Inferência:
(MP): $(\alpha, \alpha \rightarrow \beta) \vdash \beta$

Se $\vdash_{mbc}$ denota a relação de consequência de mbC então obtemos, por (MP), o seguinte:

$$\circ\alpha, \alpha, \neg\alpha \vdash_{mbc} \beta$$

Ou seja, "se α é consistente e contraditória então ela explode".

Até o momento não trabalhamos com a noção de **inconsistência** cujo símbolo representacional é $\bullet$. Para tanto, necessitaremos de definição de *negação complementar* e de *partícula bottom*.

Uma fórmula η em **L** é uma *partícula bottom* se ela pode, por si mesmo, trivializar a lógica, ou seja:

$$\forall\Gamma\forall\beta(\Gamma, \eta \vdash \beta).$$

Representaremos a partícula bottom pelo símbolo $\bot$, quando ela existir. A existência de partículas bottom em um dado sistema lógico **L** é regulamentado pelo seguinte princípio:

Princípio do *Ex Falso Sequiter Quodlibet*

$$\exists\eta\forall\Gamma\forall\beta(\Gamma, \eta \vdash \beta) \text{ (}\mathbf{L}\text{ tem uma partícula bottom).}$$

O dual da partícula bottom é a *partícula top*, $\top$, o qual trata-se de uma fórmula μ que segue de toda a teoria, ou seja:

$$\forall\Gamma(\Gamma \vdash \mu)$$

Neste momento, podemos definir a *negação complementar*.

Definição 2.3.2. Um lógica **L** tem uma *negação complementar* se existe uma fórmula $\varphi(p_0)$ tal que:
(a) $\varphi(\alpha)$ não é uma partícula bottom, para algum α.
(b) $\forall\Gamma\forall\alpha\forall\beta(\Gamma, \alpha, \varphi(\alpha) \vdash \beta)$.

Em se tratando da negação complementar para a lógica mbC, consideremos uma negação "ɾ" definida por:

$$ɾ\alpha =_{def} (\neg\alpha \wedge \circ\alpha)$$

Assim,

$$\bot_\beta =_{def} (\beta \wedge ɾ\beta), \text{ para qualquer } \beta.$$

Se, $(\sim \alpha =_{def} \alpha \to \bot_\alpha)$, então:

- Para qualquer α e β, $(\alpha, ɾ\alpha \vdash_{mbC} \beta)$
- Para qualquer α e β, $(\alpha, \sim \alpha \vdash_{mbC} \beta)$

Consideremos então um sistema com uma negação complementar $\sim$. Paralelamente à definição de contrariedade em relação a negação $\neg$, podemos definir uma teoria Γ contraditória em relação a negação $\sim$ do seguinte modo:

$$\exists\alpha(\Gamma \vdash \alpha \text{ e } \Gamma \vdash \sim \alpha)$$

As principais lógicas paraconsistentes que apresentaremos nessa tese, tal como a mbC, são todas equipadas com negações complementares. Isso permite que alguns sistemas paraconsistentes sejam capazes de simular a negação clássica.

Logo, seja $\sim$ uma *negação complementar* para o sistema mbC definida por:

$$\sim \alpha =^{def} \alpha \rightarrow \bot$$

Claramente, $\forall\alpha\forall\beta(\alpha, \sim \alpha \vdash_{mbC} \beta)$ e $\sim$ define uma *negação clássica*.

Definição 2.3.3. O operador de **inconsistência** em mbC é dado por:

$$\bullet\alpha =^{def} \sim \circ\alpha, \text{ sendo } \sim \text{ a negação clássica.}$$

Apresentaremos alguns teoremas da lógica mbC cujas demonstrações serão realizadas na próxima seção pelo método de Anéis de Polinômios.

Teorema 2.3.4. *As seguintes regras de redução são válidas em mbC:*
(i) $(\Gamma \vdash_{mbC} \circ\alpha)$, $(\Delta, \beta \vdash_{mbC} \alpha)$, $(\Lambda, \beta \vdash_{mbC} \neg\alpha)$ *implica* $(\Gamma, \Delta, \Lambda \vdash_{mbC} \neg\beta)$.
(ii) $(\Gamma \vdash_{mbC} \circ\alpha)$, $(\Delta, \neg\beta \vdash_{mbC} \alpha)$, $(\Lambda, \neg\beta \vdash_{mbC} \neg\alpha)$ *implica* $(\Gamma, \Delta, \Lambda \vdash_{mbC} \beta)$.
As seguintes regras de contraposição são válidas em mbC:
(iii) $\circ\beta, (\alpha \rightarrow \beta) \vdash_{mbC} (\neg\beta \rightarrow \neg\alpha)$.
(iv) $\circ\beta, (\alpha \rightarrow \neg\beta) \vdash_{mbC} (\beta \rightarrow \neg\alpha)$.
(v) $\circ\beta, (\neg\alpha \rightarrow \beta) \vdash_{mbC} (\neg\beta \rightarrow \alpha)$.
(vi) $\circ\beta, (\neg\alpha \rightarrow \neg\beta) \vdash_{mbC} (\beta \rightarrow \alpha)$.

Teorema 2.3.5. *Em mbC as seguintes derivações são válidas:*
(i) $\alpha, \neg\alpha \vdash_{mbC} \neg \circ \alpha$.
(ii) $(\alpha \wedge \neg\alpha) \vdash_{mbC} \neg \circ \alpha$.
(iii) $\circ\alpha \vdash_{mbC} \neg(\alpha \wedge \neg\alpha)$.
(iv) $\circ\alpha \vdash_{mbC} \neg(\neg\alpha \wedge \alpha)$.

Observação 2.3.6. A recíproca dessas condições são inválidas em mbC.

Para o próximo teorema precisaremos do conceito de *equivalência* entre conjuntos de fórmulas. Logo, Γ e Δ são *equivalentes* se:

$$\forall\alpha \in \Delta(\Gamma \vdash \alpha) \text{ e } \forall\alpha \in \Gamma(\Delta \vdash \alpha)$$

Em particular dizemos que duas fórmula α e β são equivalentes, $\alpha \equiv \beta$, se os conjuntos $\{\alpha\}$ e $\{\beta\}$ são equivalentes, ou seja:

$$(\alpha \vdash \beta) \text{ e } (\beta \vdash \alpha)$$

Teorema 2.3.7. *Em mbC temos:*
(i)$(\alpha \wedge \beta) \equiv (\beta \wedge \alpha)$, *mas* $\neg(\alpha \wedge \beta) \not\equiv \neg(\beta \wedge \alpha)$;
(ii)$(\alpha \vee \beta) \equiv (\beta \vee \alpha)$, *mas* $\neg(\alpha \vee \beta) \not\equiv \neg(\beta \vee \alpha)$;
(iii)$(\alpha \wedge \neg\alpha) \equiv (\neg\alpha \wedge \alpha)$, *mas* $\neg(\alpha \wedge \neg\alpha) \not\equiv \neg(\neg\alpha \wedge \alpha)$
(iv) $(\eta \vee \neg\eta)$ *é uma partícula top, assim* $(\alpha \vee \neg\alpha) \equiv (\beta \vee \neg\beta)$, *mas* $\neg(\alpha \vee \neg\alpha) \not\equiv \neg(\beta \vee \neg\beta)$

Este teorema nos mostra que a lógica mbC falha a respeito da *Propriedade da Substituição*, a qual diz que para toda fórmula $\varphi(p_0, ..., p_n)$, $\alpha_0, ..., \alpha_n$ e $\beta_0, ..., \beta_n$, temos:
(RP) $(\alpha_0 \equiv \beta_0)$ e $(\alpha_n \equiv \beta_n)$ implica que $\varphi(\alpha_0, ..., \alpha_n) \equiv \varphi(\beta_0, ..., \beta_n)$.

Diante disso, em mbC, **não** podemos derivar $(\neg\alpha \equiv \neg\beta)$ de $(\alpha \equiv \beta)$.

2.3.1 A semântica diádica da lógica mbC

Classicamente, temos que o valor de verdade de uma fórmula complexa do tipo $\circledast(\varphi_1, ..., \varphi_n)$, sob alguma valoração, depende do valor de verdade de suas subfórmulas imediatas. No caso em que isto ocorre para todas as fórmulas de uma dada estrutura lógica $\mathcal{L}$, dizemos que esta lógica tem uma semântica verofuncional *matricial*(ou *tabular*).

Até o momento nada foi dito a respeito de valorações e atribuições de verdade. Ocorre que, em termos de semântica, a maioria das lógicas paraconsistentes não são finito-valoradas, ou seja, não são caracterizáveis por matrizes finito valoradas. Em ((Carnielli et al. 2007), teorema 3.36, p. 32), os autores demonstram o teorema da falibilidade do sistema mbC em relação às matrizes finito valoradas e verofuncionais, e apresentam uma nova semântica semi-verofuncional adequada a esse sistema. O interessante é que essa nova semântica além de permitir interpretações para situações tidas como contraditórias, também oferece uma explicação para cenários de conflitos.

O nosso interesse é, a partir dessa semântica semi-verofuncional, apresentar algumas lógicas paraconsistentes em termos do método de provas de anéis de polinômios, o qual explicitará em sua composição a perda da verofuncionalidade dos sistemas.

Definição 2.3.8. Consideremos $\mathcal{V} = \{0, 1\}$ como um conjunto de valores de verdade, onde 1 denota o valor *verdadeiro* e 0 denota o valor *falso*. Uma mbC-valoração é qualquer função $v : For^{\circ} \to \{0, 1\}$ que satisfaz as seguintes condições:
(v1) $v(\alpha \wedge \beta) = 1$ sse $v(\alpha) = 1$ e $v(\beta) = 1$.
(v2) $v(\alpha \vee \beta) = 1$ sse $v(\alpha) = 1$ ou $v(\beta) = 1$.
(v3) $v(\alpha \to \beta) = 1$ sse $v(\alpha) = 0$ ou $v(\beta) = 1$.
(v4) $v(\neg\alpha) = 0$ implica que $v(\alpha) = 1$.
(v5) $v(\circ\alpha) = 1$ implica que $v(\alpha) = 0$ ou $v(\neg\alpha) = 0$.

Para um conjunto $\Gamma \cup \{\alpha\}$ de fórmulas de mbC, $\Gamma \Vdash_{mbC} \alpha$ significa que à fórmula α é atribuido o valor 1 para toda mbC valoração, a qual também atribuiu o valor 1 a todos os elementos de Γ.

Para maiores detalhes sobre essa semântica semi-verofuncional, bem como os teoremas de correção e completude para mbC, ver (Carnielli et al. 2007).

2.3.2 O Método de Anéis de Polinômios para a lógica mbC

Analisando com acuidade a semântica semi-verofuncional apresentada na seção anterior para mbC notamos que, o cerne do problema da não caracterização do sistema em termos de matrizes finitárias ocorre em função das cláusulas da definição de valoração do operador da negação e, consequentemente, o mesmo ocorre com o operador de consistência.

A valoração a respeito do operador para a negação nos evidencia a seguinte característica: só há informação precisa a respeito do valor de verdade quando a negação de uma dada fórmula α é falsa, ou seja:

$$v(\neg\alpha) = 0 \Rightarrow v(\alpha) = 1.$$

No entanto, nada podemos afirmar sobre o contrário, quando $v(\neg\alpha) = 1$. Nesta situação, $v(\alpha) = 1$ ou $v(\alpha) = 0$. Diante disso, o polinômio a ser desenvolvido para o operador de negação em mbC precisa caracterizar tal situação. Logo, quando não houver uma cláusula de valoração para um específico conectivo, em relação a um dos valores de verdade do sistema, definiremos que a valoração está *indeterminada* nessa situação.

Portanto, a partir de tais condições, definiremos um sistema de polinômios para mbC através de traduções das fórmulas de mbC em polinômios no Anel $\mathbb{Z}_2[X \cup X']$, sendo X' uma nova coleção de variáveis, disjunta de X, em que para cada fórmula α de mbC, atribui-se uma nova variável oculta x_α em X'. Assim, temos:

Definição 2.3.9. Sejam $X = \{x_{p_1}, x_{p_2}, ...\}$ e $X' = \{x_{\alpha_1}, x_{\alpha_2}, ...\}$ conjuntos disjuntos de variáveis algébricas, indexadas por variáveis proposicionais p_1 e por fórmulas de mbC denotadas por α_i, respectivamente. As variáveis em X' são chamadas de variáveis ocultas. O CAP para mbC é definido pela função de tradução $*$ definida por:

$$* : For_{mbC} \to \mathbb{Z}_2[X \cup X']$$

tal que:

1. $(p_i)^* = x_i$, para $x_i \in X$, p atômico.

2. $(\alpha \wedge \beta)^* = \alpha^*\beta^*$.

3. $(\alpha \vee \beta)^* = \alpha^*\beta^* + \alpha^* + \beta^*$.

4. $(\alpha \to \beta)^* = \alpha^*\beta^* + \alpha^* + 1$.

5. $(\neg\alpha)^* = \alpha^* x_\alpha + 1$, onde x_α é um termo oculto em X'.

6. $(\circ\alpha)^* = (\alpha^*(x_\alpha + 1) + 1)\, x_\alpha$, onde x_α é um termo oculto em X'.

Analisando o polinômio para a negação observamos que, de fato, sua definição está coerente com a cláusula (v_4) de valoração para a negação, pois como $(\neg\alpha)^* = \alpha^* x_\alpha + 1$, onde x_α é uma variável oculta e v se escreve como $v = I_0()^*$, para algum homomorfismo $I : \mathbb{Z}_2[X \cup X'] \to \mathbb{Z}_2$, então:

$v(\neg\alpha) = 0 \Rightarrow I(\alpha^* x_\alpha + 1) = 0 \Rightarrow I(\alpha^* x_\alpha) = 1$. Logo, $I(\alpha^*) = 1$ e $I(x_\alpha) = 1$. Assim, $v(\alpha) = 1$ e $I(x_\alpha) = 1$.

$v(\neg\alpha) = 1 \Rightarrow I(\alpha^* x_\alpha + 1) = 1 \Rightarrow I(\alpha^* x_\alpha) = 0 \Rightarrow I(\alpha^*) = 0$ ou $I(x_\alpha) = 0$. Isto significa que o valor de $I(\alpha^*)$ depende do valor de verdade da variável oculta x_α. Assim, $v(\alpha) = 0$ ou $I(x_\alpha) = 0$. Consequentemente, α pode receber tanto o valor de verdade 0 quanto 1, quando $I(x_\alpha) = 0$.

Observação análoga vale para o operador de consistência $\circ$.

Definição 2.3.10. (Relação de consequência para mbC). Para $\Gamma \cup \{\alpha\}$ fórmulas de mbC, α é uma mbC- consequência de Γ (denotado por $\Gamma \not\approx_{mbC} \alpha$) se $\gamma^*[X] \in D$ para toda $\gamma \in \Gamma$ implica que $\alpha^*[X] \in D$. Neste caso, como $D = \{1\}$, então $\alpha^* \approx 1$.

Como conseqüência de que as mbC-valorações constituem uma semântica correta e completa para mbC, ver (Carnielli 2005a), e da definição da função $*$, obtém-se o seguinte teorema:

Teorema 2.3.11. $\vdash_{mbC} \alpha$ *se, e somente se,* $\not\approx_{mbC} \alpha$.

Exemplo 2.3.12. $((\alpha \wedge \neg\alpha) \rightarrow \neg \circ \alpha)$ é um teorema em mbC.

$$((\alpha \wedge \neg\alpha) \rightarrow \neg \circ \alpha)^* \approx (\alpha \wedge \neg\alpha)^*[(\neg \circ \alpha)^* + 1] + 1$$

$$\approx \alpha^*.(\alpha^* x_\alpha + 1).[((\circ\alpha)^*.x_{\circ\alpha} + 1) + 1] + 1$$

$$\approx (\alpha^*.x_\alpha + \alpha^*).[(\alpha^*(x_\alpha + 1) + 1)x_\alpha x_{\circ\alpha}] + 1$$

$$\approx (\alpha^*.x_\alpha + \alpha^*).(\alpha^* x_\alpha + \alpha^* + 1)x_\alpha x_{\circ\alpha} + 1$$

$$\approx (\alpha^*.x_\alpha + \alpha^*).(\alpha^* x_\alpha x_\alpha x_{\circ\alpha} + \alpha^* x_\alpha x_{\circ\alpha} + x_\alpha x_{\circ\alpha}) + 1$$

$$\approx {}^2(\alpha^*.x_\alpha + \alpha^*).(x_\alpha x_{\circ\alpha}) + 1$$

$$\approx_{distrib} (\alpha^* x_\alpha x_{\circ\alpha} + \alpha^*.x_\alpha x_{\circ\alpha}) + 1$$

$$\approx 0 + 1$$

$$\approx 1$$

Observação 2.3.13. É importante salientarmos que, na lógica mbC, $\circ\alpha$ **não é equivalente** a $\neg(\alpha \wedge \neg\alpha)$. Veremos em um dos teoremas do sistema mbC que apenas um lado dessa bi-implicação é válida. Isso reflete nos polinômios pois, de fato, os polinômios para $\circ\alpha$ e $\neg(\alpha \wedge \neg\alpha)$ não coincidem.

[2] Lei do índice em $\mathbb{Z}_2$

Precisamos demonstrar que esses polinômios traduzem as valorações para mbC assim como, as valorações de mbC são traduzidas nos respectivos polinômios. Logo:

Teorema 2.3.14. *Para cada valoração v definimos, como no caso clássico (vide definição 1.3.6, p. 26), uma interpretação $I : \mathbb{Z}_2[X \cup X'] \to \mathbb{Z}_2$ como um homomorfismo de anéis tal que $v = I_0()^*$, isto é, $v(\alpha) = I(\alpha^*)$. Então, para toda sentença α em mbC,*

$$v(\alpha) = \begin{cases} \mathbf{1}(indeterminada), & sse\ I(\alpha^*) = 1(indeterminada) \\ \mathbf{0}(indeterminada), & sse\ I(\alpha^*) = 0(indeterminada) \end{cases} \tag{2.1}$$

Dizemos que $v(\alpha)$ ou $I(\alpha^*)$ é *indeterminada* quando seu valor não está determinado por suas subfórmulas imediatas. Neste contexto, a prova do teorema é dada por:

Demonstração: (Esquemática) Dado que $\Sigma^\circ = \{\wedge, \vee, \to, \neg, \circ\}$ é a assinatura da lógica mbC, precisaremos analisar se o polinômio definido para cada um dos conectivos de Σ°, caracteriza a mbC valoração do conectivo em questão. Assim, definindo $I : \mathbb{Z}_2[X \cup X'] \to \mathbb{Z}_2$ como um homomorfismo tal que:

$$I(x_p) = v(p), \text{ para } p \text{ atômica.}$$

Demonstraremos, por indução na complexidade das fórmulas, que $v = I_0()^*$.

1. Para o operador da conjunção: $(\alpha \wedge \beta)^* = \alpha^*.\beta^*$.
   (i) $I\,(\alpha \wedge \beta)^* = 1 \Leftrightarrow I(\alpha^*.\beta^*) = 1 \Leftrightarrow (I(\alpha^*) = 1, I(\beta^*) = 1)$. Por H.I, $v(\alpha) = 1$ e $v(\beta) = 1$. Então, $v(\alpha \wedge \beta) = 1$.

   (ii)$I\,(\alpha \wedge \beta)^* = 0 \Leftrightarrow I(\alpha^*.\beta^*) = 0 \Leftrightarrow I(\alpha^*) = 0$ ou $I(\beta^*) = 0$. Por H.I, $v(\alpha) = 0$ ou $v(\beta) = 0$. Então, $v(\alpha \wedge \beta) = 0$.

   Logo, $I(\alpha \wedge \beta)^* = v(\alpha \wedge \beta)$.

2. Para o operador da disjunção: $(\alpha \vee \beta)^* = \alpha^*.\beta^* + \alpha^* + \beta^*$.
   (i) $I\,(\alpha \vee \beta)^* = 1 \Leftrightarrow I(\alpha^*.\beta^* + \alpha^* + \beta^*) = 1 \Leftrightarrow I(\alpha^*) = 1$ ou $I(\beta^*) = 1$, pois:
   (a) Se $I(\alpha^*) = 1$, temos:
   $I(\beta^*) + 1 + I(\beta^*) = 1 \Rightarrow 1 = 1$.
   (b) Se $I(\beta^*) = 1$, temos:
   $I(\alpha^*) + I(\alpha^*) + 1 = 1 \Rightarrow 1 = 1$.
   Logo, por H.I, $v(\alpha) = 1$ ou $v(\beta) = 1$. Portanto, $v(\alpha \vee \beta) = 1$.
   (ii)$I\,(\alpha \vee \beta)^* = 0 \Leftrightarrow I(\alpha^*.\beta^* + \alpha^* + \beta^*) = 0 \Leftrightarrow I(\alpha^*) = 0$ e $I(\beta^*) = 0$. Logo, H.I, $v(\alpha) = 0$ e $v(\beta) = 0$. Portanto, $v(\alpha \vee \beta) = 0$.

   Sendo assim, $I(\alpha \vee \beta)^* = v(\alpha \vee \beta)$.

3. Para o operador do condicional: $(\alpha \to \beta)^* = \alpha^*.\beta^* + \alpha^* + 1$.
   (i) $I\,(\alpha \to \beta)^* = 1 \Leftrightarrow I(\alpha^*.\beta^* + \alpha^* + 1) = 1 \Leftrightarrow I(\alpha^*.\beta^* + \alpha^*) = 0 \Leftrightarrow I(\alpha^*(\beta^* + 1)) = 0 \Leftrightarrow I(\alpha^*) = 0$ ou $I(\beta^* + 1) = 0 \Leftrightarrow I(\alpha^*) = 0$ ou $I(\beta^*) = 1$. Portanto, pela H.I, $v(\alpha) = 0$ ou $v(\beta) = 1$, isto é, $v(\alpha \to \beta) = 1$.

(ii)$I\left(\alpha \rightarrow \beta\right)^{*} = 0 \Leftrightarrow I(\alpha^{*}.\beta^{*} + \alpha^{*} + 1) = 0 \Leftrightarrow I(\alpha^{*}.\beta^{*} + \alpha^{*}) = 1 \Leftrightarrow I(\alpha^{*}) = 1$ e $I(\beta^{*}) = 0$. Logo, pela H.I, $v(\alpha) = 1$ e $v(\beta) = 0$ e, portanto, $v(\alpha \rightarrow \beta) = 0$.

Assim, $I(\alpha \rightarrow \beta)^{*} = v(\alpha \rightarrow \beta)$.

4. Para o operador da negação: $(\neg\alpha)^{*} = \alpha^{*}x_{\alpha} + 1$.
(i) $I\left(\neg\alpha\right)^{*} = 0 \Leftrightarrow I(\alpha^{*}x_{\alpha} + 1) = 0 \Leftrightarrow I(\alpha^{*}x_{\alpha}) = 1 \Leftrightarrow I(\alpha^{*}) = 1$ e $I(x_{\alpha}) = 1$. Portanto, $v(\alpha) = 1$, independente do valor da variável oculta, que neste caso fica determinada com valor 1.

(ii) $I\left(\neg\alpha\right)^{*} = 1 \Leftrightarrow I(\alpha^{*}x_{\alpha} + 1) = 1 \Leftrightarrow I(\alpha^{*}x_{\alpha}) = 0 \Leftrightarrow I(\alpha^{*}) = 0$ ou $I(x_{\alpha}) = 0$. Diante disso, o valor de α depende da variável oculta. Portanto, se $I(x_{\alpha}) = 0$, então $v(\alpha) = 1$ ou $v(\alpha) = 0$, ou seja, é indeterminado o valor de α.

Assim, recuperamos apenas a implicação $v(\neg\alpha) = 0 \Rightarrow v(\alpha) = 1$.

5. Para o operador da consistência: $(\circ\alpha)^{*} = \left(\alpha^{*}\left(x_{\alpha} + 1\right) + 1\right)x_{\alpha}$.

(i) $I\left(\circ\alpha\right)^{*} = 1 \Leftrightarrow I(\left(\alpha^{*}\left(x_{\alpha} + 1\right) + 1\right)x_{\alpha}) = 1 \Leftrightarrow I(x_{\alpha}) = 1$ e $I(\alpha^{*}\left(x_{\alpha} + 1\right) + 1) = 1$. Logo, $I(\alpha^{*}\left(x_{\alpha} + 1\right)) = 0 \Leftrightarrow I(\alpha^{*}) = 0$ ou $I(x_{\alpha}) = 1$.
(a) Se $I(\alpha^{*}) = 0$, contemplamos a primeira cláusula da valoração (v_5), ou seja, $v(\alpha) = 0$.
(b) Se $I(x_{\alpha}) = 1$, então:

$$(\neg\alpha)^{*} = \alpha^{*}x_{\alpha} + 1, \text{ torna-se } (\neg\alpha)^{*} = \alpha^{*} + 1.$$

Assim:
Se $I(\alpha^{*}) = 0$, temos a primeira cláusula da valoração.
Se $I(\alpha^{*}) = 1$, então, $I((\neg\alpha)^{*}) = 1 + 1 = 0$, ou seja, $v(\neg\alpha) = 0$ e contemplamos a segunda cláusula da valoração (v_5), isto é, $I(\neg\alpha)^{*} = 0$ e $v(\neg\alpha) = 0$.

(ii) $I\left(\circ\alpha\right)^{*} = 0 \Rightarrow I(\left(\alpha^{*}\left(x_{\alpha} + 1\right) + 1\right)x_{\alpha}) = 0 \Rightarrow I(x_{\alpha}) = 0$ ou $I(\alpha^{*}\left(x_{\alpha} + 1\right) + 1) = 0 \Leftrightarrow I(\alpha^{*}\left(x_{\alpha} + 1\right)) = 1 \Leftrightarrow I(\alpha^{*}) = 1$ e $I(x_{\alpha}) = 0$. Diante disso, o valor de verdade de $(\circ\alpha)^{*}$ depende do valor de verdade da variável oculta, pois para $I(x_{\alpha}) = 0$, $v(\alpha) = 1$ ou $v(\alpha) = 0$.

Assim, recuperamos apenas a implicação: $v(\circ\alpha) = 1 \Rightarrow v(\alpha) = 0$ ou $v(\neg\alpha) = 0$.

■

O teorema 2.3.14 mostra que, de fato, a tradução da definição 2.3.9 garante um tratamento polinomial correto e completo em $\mathbb{Z}_2[X \cup X']$ para a lógica mbC.

Teorema 2.3.15. *Para todo homomorfismo $I : \mathbb{Z}_2[X \cup X'] \rightarrow \mathbb{Z}_2$, $I_0()^{*}$ é uma valoração.*

Demonstração: Consideremos a valoração v definida por $v : For^{\circ} \rightarrow \{0, 1\}$ (como definida em 2.3.8, p. 46). Se I é um homomorfismo, $I : \mathbb{Z}_2[X \cup X'] \rightarrow \mathbb{Z}_2$ tal que para todo p, atômico, $v(p) = I(p)^{*}$ e para toda fórmula φ, $\varphi \in For^{\circ}$, $v(\varphi) = I(\varphi)^{*}$, então $v = I_0()^{*}$. Por 2.3.14, de fato temos que $v = I_0()^{*}$ para a lógica mbC. Portanto, $I_0()^{*}$ é uma valoração. ■

Alguns teoremas a respeito de mbC foram apresentados mas não demonstrados, na seção precedente. À guisa de exemplos de aplicações do método, vamos demonstrá-los utilizando anéis de polinômios.

Teorema 2.3.16. *As seguintes regras de contraposição são válidas em mbC:*
(i) $\circ\beta, (\alpha \to \beta) \vdash_{mbC} (\neg\beta \to \neg\alpha)$.
(ii) $\circ\beta, (\alpha \to \neg\beta) \vdash_{mbC} (\beta \to \neg\alpha)$.
(iii) $\circ\beta, (\neg\alpha \to \beta) \vdash_{mbC} (\neg\beta \to \alpha)$.
(iv) $\circ\beta, (\neg\alpha \to \neg\beta) \vdash_{mbC} (\beta \to \alpha)$.

Demonstração: [3]
(i) Consideremos que $v(\circ\beta) = 1$, $v(\alpha \to \beta) = 1$ e $v(\neg\beta \to \neg\alpha) = 0$. Aplicando o método de polinômios temos que:

1. $v(\circ\beta) = 1$
   $v(\circ\beta) = 1 \Leftrightarrow I((\beta^* (x_\beta + 1) + 1)\, x_\beta) = 1 \Rightarrow I(x_\beta) = 1$ e $I((\beta^* (x_\beta + 1) + 1)) = 1 \Leftrightarrow I(x_\beta) = 1$ e $I(\beta^* (x_\beta + 1)) = 0 \Leftrightarrow I(x_\beta) = 1$ e $[I(\beta^* = 0)$ ou $I(x_\beta) = 1]$
   Pela regra da absorção $(\varphi \wedge (\psi \vee \varphi) \Rightarrow \varphi)$, temos:
   $v(\circ\beta) = 1 \Rightarrow I(x_\beta) = 1$.

2. $v(\alpha \to \beta) = 1$
   $v(\alpha \to \beta) = 1 \Leftrightarrow I(\alpha^*\beta^* + \alpha^* + 1) = 1 \Leftrightarrow I(\alpha^*(\beta^* + 1)) = 0 \Leftrightarrow I(\alpha^*) = 0$ ou $I(\beta^*) = 1$.
   Logo, $v(\alpha) = 0$ ou $v(\beta) = 1$. Portanto:
   $v(\alpha \to \beta) = 1 \Rightarrow v(\alpha) = 0$ ou $v(\beta) = 1$.

   Dos itens (1) e (2) podemos concluir que, para ambas as cláusulas serem verdadeiras, devemos ter:

   (a) $I(x_\beta) = 1$ e $(v(\alpha) = 0 \vee v(\beta) = 1)$

$$I : I(x_\beta) = 1, v(\alpha) = 0$$

ou

$$II : I(x_\beta) = 1, v(\beta) = 1$$

Em uma dedução, premissas verdadeiras acarretam em uma conclusão necessariamente verdadeira. Assim, ao considerarmos as premissas verdadeiras e a conclusão falsa, devemos chegar a um resultado absurdo.

Suponhamos que $v(\neg\beta \to \neg\alpha) = 0$. Então:
$v(\neg\beta \to \neg\alpha) = 0 \Leftrightarrow I((\beta^* x_\beta + 1)(\alpha^* x_\alpha) + 1) = 0 \Leftrightarrow I(\beta^* x_\beta + 1) = 1$ e $I(\alpha^* x_\alpha) = 1 \Leftrightarrow I(\beta^* x_\beta) = 0$ e $I(\alpha^* x_\alpha) = 1 \Leftrightarrow I(\beta^*) = 0$ ou $I(x_\beta) = 0$ e $I(\alpha^*) = 1$ e $I(x_\alpha) = 1$. Isso implica que:

$$III : v(\beta) = 0, v(\alpha) = 1, I(x_\alpha) = 1$$

ou

$$IV : I(x_\beta) = 0, v(\alpha) = 1, I(x_\alpha) = 1$$

Assim, por redução ao absurdo, temos:

[3] A partir de agora aplicaremos, constantemente, o teorema 2.3.14 sem o mencionarmos a todo momento.

- Se $v(\neg\beta \rightarrow \neg\alpha) = 0$, temos que: I é incompatível com III e IV. Analogamente, II é incompatível com III e IV.

(ii) $\circ\beta, (\alpha \rightarrow \neg\beta) \vdash_{mbC} (\beta \rightarrow \neg\alpha)$.

Consideremos que $v(\circ\beta) = 1$, $v(\alpha \rightarrow \neg\beta) = 1$ e $v(\beta \rightarrow \neg\alpha) = 0$.

1. $v(\circ\beta) = 1$.
   Pelo item (1) na prova de (i) temos que:
   $v(\circ\beta) = 1 \Rightarrow I(x_\beta) = 1$.

2. $v(\alpha \rightarrow \neg\beta) = 1$.
   $v(\alpha \rightarrow \neg\beta) = 1 \Leftrightarrow I(\alpha^*(\beta^* x_\beta) + 1) = 1 \Leftrightarrow I(\alpha^*(\beta^* x_\beta)) = 0 \Leftrightarrow I(\alpha^*) = 0$ ou $I(\beta^*) = 0$ ou $I(x_\beta) = 0$. Isto é:
   $v(\alpha \rightarrow \neg\beta) = 1 \Rightarrow v(\alpha) = 0$ ou $v(\beta) = 0$ ou $I(x_\beta) = 0$

   Dos itens (1) e (2) podemos concluir que, para ambas as cláusulas serem verdadeiras, devemos ter:

   (a) $v(\alpha) = 0, I(x_\beta) = 1$ ou

   (b) $v(\beta) = 0, I(x_\beta) = 1$.

Supondo, por redução ao absurdo, que $v(\beta \rightarrow \neg\alpha) = 0$. Então:
$v(\beta \rightarrow \neg\alpha) = 0 \Leftrightarrow I(\beta^*.(\alpha^*.x_\alpha) + 1) = 0 \Leftrightarrow I(\beta^*.(\alpha^*.x_\alpha)) = 1 \Leftrightarrow I(\beta^*) = 1$ e $I(\alpha^*) = 1$ e $I(x_\alpha) = 1$.

Logo, $(\beta \rightarrow \neg\alpha) = 0 \Rightarrow v(\beta) = 1, v(\alpha) = 1, I(x_\alpha) = 1$.

Se $v(\beta) = 1$, há uma contradição com (b). Analogamente, se $v(\alpha) = 1$, então temos uma contradição com (a).

(iii) $\circ\beta, (\neg\alpha \rightarrow \beta) \vdash_{mbC} (\neg\beta \rightarrow \alpha)$.
Consideremos que $v(\circ\beta) = 1$, $v(\neg\alpha \rightarrow \beta) = 1$ e $v(\neg\beta \rightarrow \alpha) = 0$. Aplicando os polinômios temos que:

1. $v(\circ\beta) = 1$.
   Pelo item (1) na prova de (i) temos que:
   $v(\circ\beta) = 1 \Rightarrow I(x_\beta) = 1$.

2. $v(\neg\alpha \rightarrow \beta) = 1$.
   $v(\neg\alpha \rightarrow \beta) = 1 \Leftrightarrow I((\alpha^* x_\alpha + 1)(\beta^* + 1) + 1) = 1 \Leftrightarrow I((\alpha^* x_\alpha + 1)(\beta^* + 1)) = 0 \Leftrightarrow I(\alpha^* x_\alpha + 1) = 0$ ou $I(\beta^* + 1) = 1 \Leftrightarrow (I(\alpha^*) = 1$ e $I(x_\alpha) = 1)$ ou $I(\beta^*) = 1$.

   Dos itens (1) e (2) podemos concluir que, para ambas as cláusulas serem verdadeiras, devemos ter:

   (a) $I(x_\beta) = 1, v(\alpha) = 1, I(x_\alpha) = 1$, ou

   (b) $I(x_\beta) = 1, v(\beta) = 1$

Supondo, por redução ao absurdo que $v(\neg\beta \rightarrow \alpha) = 0$, temos:
$v(\neg\beta \rightarrow \alpha) = 0 \Leftrightarrow I((\beta^* x_\beta + 1)(\alpha^* + 1) + 1) = 0 \Leftrightarrow I((\beta^* x_\beta + 1)(\alpha^* + 1)) = 1 \Leftrightarrow I(\beta^* x_\beta + 1) = 1$ e $I(\alpha^* + 1) = 1 \Leftrightarrow I(\beta^*) = 0$ ou $I(x_\beta) = 0$ e $I(\alpha) = 0$. Isto é:
(c) $v(\beta) = 0$ e $v(\alpha) = 0$, ou
(d) $I(x_\beta) = 0$ e $v(\alpha) = 0$.

Assim, (c) contradiz (a) e (b) e (d) também contradiz (a) e (b).

(iv) $\circ\beta, (\neg\alpha \rightarrow \neg\beta) \vdash_{mbC} (\beta \rightarrow \alpha)$.
Consideremos que $v(\circ\beta) = 1$, $v(\neg\alpha \rightarrow \neg\beta) = 1$ e $v(\beta \rightarrow \alpha) = 0$. Aplicando os polinômios temos que:

1. $v(\circ\beta) = 1$.
   Pelo item (1) na prova de (i) temos que:
   $v(\circ\beta) = 1 \Rightarrow I(x_\beta) = 1$.

2. $v(\neg\alpha \rightarrow \neg\beta) = 1$.
   $v(\neg\alpha \rightarrow \neg\beta) = 1 \Leftrightarrow I((\alpha^* x_\alpha + 1)(\beta^* x_\beta) + 1) = 1 \Leftrightarrow (I(\alpha^*) = 1$ e $I(x_\alpha) = 1)$ ou $I(\beta^*) = 0$ ou $I(x_\beta) = 0$.

   Dos itens (1) e (2) podemos concluir que, para ambas as cláusulas serem verdadeiras, devemos ter:

   (a) $I(x_\beta) = 1, v(\alpha) = 1, I(x_\alpha) = 1$, ou

   (b) $I(x_\beta) = 1, v(\beta) = 0$.

Supondo, por redução ao absurdo que $v(\beta \rightarrow \alpha) = 0$, temos:
$v(\beta \rightarrow \alpha) = 0 \Leftrightarrow I(\beta^*.\alpha^* + \beta^* + 1) = 0 \Leftrightarrow I(\beta^*) = 1$ e $I(\alpha^*) = 0$. Isto é, $v(\beta) = 1$ e $v(\alpha) = 0$, o que contradiz ambas as cláusulas (a) e (b). ∎

2.4 Uma das mais ricas LFIs: a lógica mCi.

Na seção anterior apresentamos o conceito de *negação complementar* e lembramos que em mbC:
$\wr\alpha =_{def} (\neg\alpha \wedge \circ\alpha)$
$\perp =_{def} (\alpha \wedge \wr\alpha)$
$\sim \alpha =_{def} \alpha \rightarrow \perp$
Logo:
$\sim \alpha =_{def} \alpha \rightarrow \perp =_{def} \alpha \rightarrow (\alpha \wedge \wr\alpha) =_{def} \alpha \rightarrow (\alpha \wedge (\neg\alpha \wedge \circ\alpha))$. Portanto,
$\sim \alpha = \alpha \rightarrow (\alpha \wedge (\neg\alpha \wedge \circ\alpha))$.

Assim, em mbC podemos definir o conectivo de inconsistência do seguinte modo:

$$\bullet\alpha =_{def} \sim \circ\alpha$$

onde $\sim$ é a negação clássica. No entanto, seria possível ter um sistema capaz de definir o operador de inconsistência por meio da negação paraconsistente, ou seja, um sistema em que $\bullet\alpha =_{def} \neg \circ \alpha$? A resposta é sim, e o sistema capaz de realizar isto é o mCi.

O sistema mCi é uma extensão de mbC que se caracteriza pela incorporação de novos esquemas de axiomas no escopo sintático de mbC. E conforme apresentado acima, em mCi as fórmulas $\bullet\alpha$ e $\neg \bullet \alpha$ serão logicamente indistinguíveis de $\neg \circ \alpha$ e $\circ\alpha$, isto é:

$$\bullet\alpha \equiv_{mCi} \neg \circ \alpha.$$
$$\neg \bullet \alpha \equiv_{mCi} \circ\alpha.$$

Definição 2.4.1. A lógica **mCi** é obtida a partir de mbC pela adição dos seguintes esquemas de axiomas:
(ci) $\neg \circ \alpha \rightarrow (\alpha \wedge \neg\alpha)$
$(cc)_n \circ \neg^n \circ \alpha, (n \geq 0)$.
O operador de inconsistência, $\bullet$, é definido por $\bullet\alpha \equiv_{mCi} \neg \circ \alpha$.

O primeiro esquema de axioma, (ci), advém de um teorema de mbC cuja recíproca não é demonstrável em mbC, ou seja, $(\alpha \wedge \neg\alpha) \vdash_{mbC} \neg \circ \alpha$, mas $\neg \circ \alpha \nvdash_{mbC} (\alpha \wedge \neg\alpha)$. Já o segundo, $(cc)_n$, ocorre do desejo de que fórmulas da forma $\neg\circ\alpha$ comportem-se classicamente, e da intenção de obtermos um sistema cuja explosão seja controlável quando em contato com fórmulas do tipo $\neg^n \circ \alpha$, onde:

$$\neg^n \circ \alpha = \begin{cases} \neg^0 \circ \alpha = \circ\alpha \\ \neg^{n+1} \circ \alpha = \neg\neg^n \circ \alpha \end{cases} \tag{2.2}$$

Não é difícil provar que o conjunto $\{\neg^n \circ \alpha; \neg^{n+1} \circ \alpha\}$ é explosivo em mCi, pois da união de $\{\neg^n \circ \alpha; \neg^{n+1} \circ \alpha\}$ com $(cc)_n$, obtemos:
$\{\circ\neg^n \circ \alpha; \neg^n \circ \alpha; \neg^{n+1} \circ \alpha\} =^{(1)} \{\circ\neg^n \circ \alpha; \neg^n \circ \alpha; \neg\neg^n \circ \alpha\}$.
Pelo axioma (bc1) de mbC, o qual diz que $\circ\alpha \rightarrow (\alpha \rightarrow (\neg\alpha \rightarrow \beta))$, o sistema inserido do conjunto $\{\neg^n \circ \alpha; \neg^{n+1} \circ \alpha\}$ explode, pois:
$\circ\neg^n \circ \alpha \rightarrow (\neg^n \circ \alpha \rightarrow (\neg\neg^n \circ \alpha \rightarrow \beta))$.

Os teoremas inerentes à lógica mCi serão apresentados e demonstrados via anéis de polinômios, o que veremos em uma das seções seguintes.

2.4.1 A semântica da lógica mCi

Assim como o sistema mbC, a lógica mCi não é caracterizável por matrizes finitas, conforme apresentado em (Carnielli et al. 2007), teorema 3.36, p. 32. Logo, precisamos de uma função de valoração que caracterize tal condição.

Definição 2.4.2. Uma mCi-valoração é qualquer função $v : For^\circ \rightarrow \{0, 1\}$ que satisfaz as seguintes condições:
(v1) $v(\alpha \wedge \beta) = 1$ sse $v(\alpha) = 1$ e $v(\beta) = 1$.
(v2) $v(\alpha \vee \beta) = 1$ sse $v(\alpha) = 1$ ou $v(\beta) = 1$.
(v3) $v(\alpha \rightarrow \beta) = 1$ sse $v(\alpha) = 0$ ou $v(\beta) = 1$.
(v4) $v(\neg\alpha) = 0$ implica que $v(\alpha) = 1$.
(v5) $v(\circ\alpha) = 1$ implica que $v(\alpha) = 0$ ou $v(\neg\alpha) = 0$.

(v6) $v(\neg \circ \alpha) = 1$ implica que $v(\alpha) = 1$ e $v(\neg\alpha) = 1$.
(v7) $v(\circ\neg^n \circ \alpha) = 1$ para $(n \geq 0)$.

As cláusulas (v1)-(v5) são as condições de verdade para a semântica de mbC. Apenas (v6) e (v7) dizem respeito, especificamente, à lógica mCi.

Denotaremos por $\vDash_{mCi}$ a relação de consequência semântica de mCi. Em (Carnielli et al. 2007) os autores demonstram a correção e completude das cláusulas da definição 2.4.2 para mCi.

2.4.2 Anéis de polinômios para a lógica mCi

Os polinômios a serem definidos nessa seção dizem respeito apenas as cláusulas (v6) e (v7), já que as demais foram definidas nos polinômios para mbC.

Definição 2.4.3. Definimos $*$ como uma função que traduz fórmulas de mCi em polinômios no anel $\mathbb{Z}_2[X \cup X']$, isto é:

$$* : For_{mCi} \to \mathbb{Z}_2[X \cup X']$$

tal que:
(i) $(\neg \circ \alpha)^* = (\alpha^*)(x_\alpha + 1)(x_{\circ\alpha})$, onde x_α e $x_{\circ\alpha}$ são variáveis ocultas.
Restrição: $I(x_{\circ\alpha}) = 1$.
(ii) $(\circ\neg^n \circ \alpha)^* = x_{\circ\neg^n\circ\alpha}$, onde $x_{\circ\neg^n\circ\alpha}$ é uma variável oculta.
Restrição: $I(x_{\circ\neg^n\circ\alpha}) = 1$

Observação 2.4.4. A restrição inerente ao termo oculto $I(x_{\circ\alpha}) = 1$ é decorrente do fato de que, ao pensarmos na negação da consistência em termos de fórmulas sem o operador de consistência, nos deparamos com uma negação recorrente, ou seja, $(\neg \circ \alpha)$ seria tratado como $\neg(\neg(\alpha \wedge \neg\alpha))$. Essa identificação não é válida em mCi, mas quando aplicamos as regras de obtenção do polinômio, as variáveis ocultas são as mesmas. Isso explica a restrição $I(x_{\circ\alpha}) = 1$. Uma razão análoga vale para a cláusula (ii).

Teorema 2.4.5. *Para cada valoração v definimos, como no caso clássico (vide definição 1.3.6, p. 26), uma interpretação $I : \mathbb{Z}_2[X \cup X'] \to \mathbb{Z}_2$ como um homomorfismo de anéis tal que $v = I_0()^*$, isto é, $v(\alpha) = I(\alpha^*)$. Então, para toda sentença α em mCi,*

$$v(\alpha) = \begin{cases} \textbf{\textit{1}}(indeterminada), & sse\ I(\alpha^*) = 1(indeterminada) \\ \textbf{\textit{0}}(indeterminada), & sse\ I(\alpha^*) = 0(indeterminada) \end{cases} \tag{2.3}$$

Demonstração: (Esquemática).
(i) Seja $(\alpha^*)(x_\alpha + 1)(x_{\circ\alpha})$ o polinômio que traduz as fórmulas do tipo $(\neg \circ \alpha)$.

1. $v(\neg \circ \alpha) = 1$.

   $v(\neg \circ \alpha) = 1 \Leftrightarrow I((\alpha^*)(x_\alpha + 1)(x_{\circ\alpha})) = 1 \Leftrightarrow I((\alpha^*)(x_\alpha + 1)) = 1$ e $I(x_{\circ\alpha}) = 1 \Leftrightarrow I(\alpha^*) = 1$ e $I(x_\alpha + 1) = 1$ e $I(x_{\circ\alpha}) = 1$.

Sendo assim, $v(\neg \circ \alpha) = 1 \Rightarrow v(\alpha) = 1, I(x_\alpha) = 0, I(x_{\circ\alpha}) = 1$.

Como $(\neg\alpha)^* = \alpha^*.x_\alpha + 1$, então:
$I((\neg\alpha)^*) = 0 + 1 = 1$. Portanto, $v(\neg\alpha) = 1$.

Portanto, $v(\neg \circ \alpha) = 1 \Rightarrow v(\alpha) = 1$ e $v(\neg\alpha) = 1$.

2. $v(\neg \circ \alpha) = 0$.

$v(\neg\circ\alpha) = 0 \Leftrightarrow I((\alpha^*\,(x_\alpha + 1))\,x_{\circ\alpha}) = 0 \Leftrightarrow I((\alpha^*)(x_\alpha+1)) = 0$ ou $I(x_{\circ\alpha}) = 0 \Leftrightarrow I(\alpha^*) = 0$ ou $I(x_\alpha + 1) = 0$ ou $I(x_{\circ\alpha}) = 0$.

Quando $I(x_\alpha) = 1$, $v(\alpha)$ é indeterminado, isto é, o valor de α não é determinado pelas subfórmulas imediatas.

(ii) O polinômio que interpreta a fórmula $(\circ\neg^n \circ \alpha)$ é dado por $(x_{\circ\neg^n\circ\alpha})$.

1. $I(\circ\neg^n \circ \alpha)^* = 1$
$I(\circ\neg^n \circ \alpha)^* = 1 \Rightarrow I(x_{\circ\neg^n\circ\alpha}) = 1$.

2. $v(\circ\neg^n \circ \alpha)^* = 0$
Se $I(\circ\neg^n \circ \alpha)^* = 0$, então $I(x_{\circ\neg^n\circ\alpha}) = 0$. No entanto, pela restrição, isto não é possível. Portanto, temos uma indeterminação.

■

O teorema 2.4.5 mostra que, de fato, a tradução da definição 2.4.3 garante um tratamento polinomial correto e completo, em $\mathbb{Z}_2[X \cup X']$, para a lógica mCi.

2.5 As lógicas bC, Ci, mbCe, mCie, bCe e Cie

Os sistemas bC, Ci, mbCe, mCie, bCe e Cie são extensões de mbC e mCi por meio da incorporação de esquemas de axiomas que envolvem duplas negações. Os axiomas são os seguintes:
(cf) $\neg\neg\alpha \rightarrow \alpha$.
(ce) $\alpha \rightarrow \neg\neg\alpha$.

Definição 2.5.1. Consideremos $\Sigma^\circ = \{\wedge, \vee, \rightarrow, \neg, \circ\}$. Definimos as Lógicas da Inconsistência Formal, bC e Ci, como:

- A lógica **bC** é uma extensão de mbC pela inserção do axioma (cf) em seu escopo sintático.
- **Ci** é axiomatizada como mCi, com a adição do axioma (cf).

Definição 2.5.2. Consideremos $\Sigma^\circ = \{\wedge, \vee, \rightarrow, \neg, \circ\}$. Definimos as Lógicas da Inconsistência Formal, mbCe e mCie, como:

- A lógica **mbCe** é uma extensão de mbC pela incorporação do axioma (ce).
- A lógica **mCie** é axiomatizada como mCi, com a adição o axioma (ce).

Definição 2.5.3. Consideremos $\Sigma^{\circ} = \{\wedge, \vee, \rightarrow, \neg, \circ\}$. Definimos as Lógicas da Inconsistência Formal, bCe e Cie, como:

- A lógica **bCe** é axiomatizada como bC, com a adição do axioma (ce).
- **Cie** é uma extensão Ci pela incorporação do axioma (ce).

2.5.1 A semântica dos sistemas bC, Ci, mbCe, mCie, bCe e Cie

Para estes sistemas necessitamos definir as cláusulas de valoração semântica apenas para os axiomas (cf) e (ce).

Definição 2.5.4. Definimos as cláusulas de valoração semântica correspondentes aos axiomas (cf) e (ce), respectivamente, considerando v como uma função valoração de $v : For^{\circ} \rightarrow \{0, 1\}$, como:
(v8) $v(\neg\neg\alpha) = 1$, implica que $v(\alpha) = 1$ (cf).
(v9) $v(\alpha) = 1$, implica que $v(\neg\neg\alpha) = 1$ (ce).

2.5.2 O anel de polinômios para os sistemas bC, Ci, mbCe, mCie, bCe e Cie.

Os polinômios a serem definidos nessa seção dizem respeito apenas à cláusulas (v8) e (v9), já que os demais foram definidos nos polinômios para mbC e mCi.

Definição 2.5.5. Definimos $*$ como uma função que traduz fórmulas de bC e Ci em polinômios no Anel $\mathbb{Z}_2[X \cup X']$, isto é:

$$* : For_{\{bC,Ci\}} \rightarrow \mathbb{Z}_2[X \cup X']$$

tal que:
$(\neg\neg\alpha)^* = ((\alpha^* x_\alpha + 1)x_\alpha + 1)$.

Restrição: $I(x_\alpha = 1)$.

Teorema 2.5.6. *Para cada valoração v definimos, como no caso clássico (vide definição 1.3.6, p. 26), uma interpretação $I : \mathbb{Z}_2[X \cup X'] \rightarrow \mathbb{Z}_2$ como um homomorfismo de anéis tal que $v = I_0()^*$, isto é, $v(\alpha) = I(\alpha^*)$. Então, para toda sentença α em bC e Ci,*

$$v(\alpha) = \begin{cases} \mathbf{1}(indeterminada), & sse\ I(\alpha^*) = 1(indeterminada) \\ \mathbf{0}(indeterminada), & sse\ I(\alpha^*) = 0(indeterminada) \end{cases} \tag{2.4}$$

Demonstração: (Esquemática).

(i) $v(\neg\neg\alpha) = 1$.
$v(\neg\neg\alpha) = 1 \Leftrightarrow I((\neg\neg\alpha)^*) = 1 \Leftrightarrow I((\alpha^* x_\alpha + 1)x'_\alpha + 1) = 1 \Leftrightarrow I((\alpha^* x_\alpha + 1)x'_\alpha) = 0 \Leftrightarrow I(x'_\alpha) = 0$ ou $I(\alpha^* x_\alpha + 1) = 0 \Leftrightarrow I(\alpha^* x_\alpha) = 1 \Leftrightarrow I(\alpha^*) = 1$ e $I(x_\alpha) = 1$. Concluímos que: $I(x'_\alpha) = 0$ ou ($I(\alpha^*) = 1$ e $I(x_\alpha) = 1$). Pela restrição, $I(x'_\alpha)$ não pode ter valor nulo, então, $I(\alpha^*) = 1$ e

$I(x_\alpha) = 1$. Portanto, $v(\alpha) = 1$.

(i) $v(\neg\neg\alpha) = 0$.
$v(\neg\neg\alpha) = 0 \Leftrightarrow I((\neg\neg\alpha)^*) = 0 \Leftrightarrow I(((\alpha^* x_\alpha + 1)x'_\alpha + 1)) = 0 \Leftrightarrow I((\alpha^* x_\alpha + 1)x'_\alpha) = 1 \Leftrightarrow I(x'_\alpha) = 1$ e $I(\alpha^* x_\alpha + 1) = 1 \Leftrightarrow I(x_\alpha) = 0$ ou $I(\alpha^*) = 0$. Logo, $v(\neg\neg\alpha)$ é indeterminado. ■

Definição 2.5.7. Definimos $*$ como uma função que traduz fórmulas de mbCe e mCie em polinômios no Anel $\mathbb{Z}_2[X \cup X']$, isto é:

$$* : For_{\{mbCe,mCie\}} \to \mathbb{Z}_2[X \cup X']$$

tal que:
$(\neg\neg\alpha)^* = ((\alpha^* + 1)x_\alpha + 1)$.

Teorema 2.5.8. *Para cada valoração v definimos, como no caso clássico (vide definição 1.3.6, p. 26), uma interpretação $I : \mathbb{Z}_2[X \cup X'] \to \mathbb{Z}_2$ como um homomorfismo de anéis tal que $v = I_0()^*$, isto é, $v(\alpha) = I(\alpha^*)$. Então, para toda sentença α em mbCe e mCie,*

$$v(\alpha) = \begin{cases} \mathbf{1}(indeterminada), & sse\ I(\alpha^*) = 1(indeterminada) \\ \mathbf{0}(indeterminada), & sse\ I(\alpha^*) = 0(indeterminada) \end{cases} \tag{2.5}$$

Demonstração: (Esquemática).

(i) Temos que, $I(\alpha^*) = 1$ sse $v(\alpha) = 1$.
$(\neg\neg\alpha)^* = (\alpha^* + 1)x_\alpha + 1$. Como $v(\alpha) = 1$, então:
$I((\neg\neg\alpha)^*) = I((\alpha^* + 1)x_\alpha + 1) = 0 + 1 = 1$, ou seja, $I((\neg\neg\alpha)^*) = 1$. Consequentemente, $v(\neg\neg\alpha) = 1$.

(ii) Do mesmo modo, $I(\alpha^*) = 0$ sse $v(\alpha) = 0$.
$(\neg\neg\alpha)^* = (\alpha + 1)x^*_\alpha + 1$. Como $v(\alpha) = 0$, então:
$I((\neg\neg\alpha)^*) = (0 + 1)I(x_\alpha) + 1 = I(x_\alpha) + 1$. Portanto, $I((\neg\neg\alpha)^*)$ é indeterminado e, consequentemente, $v(\neg\neg\alpha)$ é indeterminado.

■

Definição 2.5.9. Definimos $*$ como uma função que traduz fórmulas de bCe e Cie em polinômios no Anel $\mathbb{Z}_2[X \cup X']$, isto é:

$$* : For_{\{bCe,Cie\}} \to \mathbb{Z}_2[X \cup X']$$

tal que:
$(\neg\neg\alpha)^* = ((\alpha^* x_\alpha + 1)x_\alpha + 1)$.

Restrição: $I(x_\alpha) = 1$.

Teorema 2.5.10. *Para cada valoração v definimos, como no caso clássico (vide definição 1.3.6, p. 26), uma interpretação $I : \mathbb{Z}_2[X \cup X'] \to \mathbb{Z}_2$ como um homomorfismo de anéis tal que $v = I_0()^*$, isto é, $v(\alpha) = I(\alpha^*)$. Então, para toda sentença α em bCe e Cie,*

$$v(\alpha) = \begin{cases} \mathbf{1}(indeterminada), & sse\ I(\alpha^*) = 1(indeterminada) \\ \mathbf{0}(indeterminada), & sse\ I(\alpha^*) = 0(indeterminada) \end{cases} \tag{2.6}$$

Demonstração: (Esquemática).

(i) $v(\neg\neg\alpha) = 1$.
$v(\neg\neg\alpha) = 1 \Leftrightarrow I((\neg\neg\alpha)^*) = 1 \Leftrightarrow I((\alpha^* x_\alpha + 1)x_\alpha + 1) = 1 \Leftrightarrow I((\alpha^* x_\alpha + 1)x_\alpha) = 0$. Logo, $I(x_\alpha) = 0$ ou $I(\alpha^* x_\alpha + 1) = 0 \Leftrightarrow I(\alpha^* x_\alpha) = 1 \Leftrightarrow I(\alpha^*) = 1$ e $I(x_\alpha) = 1$. Concluímos que: $I(x_\alpha) = 0$ ou $(I(\alpha^*) = 1$ e $I(x_\alpha) = 1)$. Pela restrição, a primeira condição $(I(x_\alpha) = 0)$ está desconsiderada. Assim, temos que $v(\alpha) = 1$ e $I(x_\alpha) = 1$. Portanto, $v(\alpha) = 1$.

$v(\neg\neg\alpha) = 0$.
$v(\neg\neg\alpha) = 0 \Leftrightarrow I((\neg\neg\alpha)^*) = 0 \Leftrightarrow I((\alpha^* x_\alpha + 1)x_\alpha + 1) = 0 \Leftrightarrow I((\alpha^* x_\alpha + 1)x_\alpha) = 1 \Leftrightarrow I(x_\alpha) = 1$ e $I(\alpha^* x_\alpha + 1) = 1 \Leftrightarrow I(x_\alpha) = 0$ ou $I(\alpha^*) = 0$. Pela restrição, concluímos que $I(\alpha^*) = 0$ e consequentemente, $v(\alpha) = 0$.

■

Os teoremas 2.5.6, 2.5.8 e 2.5.10 mostram que, de fato, as traduções das respectivas definições 2.5.5, 2.5.7 e 2.5.9 garantem um tratamento polinomial correto e completo, em $\mathbb{Z}_2[X \cup X']$, para as lógicas bC, Ci, mbCe, mCie, bCe e Cie.

2.6 A Lógica da Inconsistência Formal LFI1

A lógica LFI1, um sistema trivalente e paraconsistente, é axiomatizada a partir da lógica Cie, por meio da inserção dos seguintes esquemas de axiomas em sua sintaxe:
(cj1): $\bullet(\alpha \wedge \beta) \leftrightarrow ((\bullet\alpha \wedge \beta) \vee (\bullet\beta \wedge \alpha))$;
(cj2): $\bullet(\alpha \vee \beta) \leftrightarrow ((\bullet\alpha \wedge \neg\beta) \vee (\bullet\beta \wedge \neg\alpha))$;
(cj3): $\bullet(\alpha \rightarrow \beta) \leftrightarrow (\alpha \wedge \bullet\beta)$.
Assim, temos:

Definição 2.6.1. Seja $\Sigma^{\bullet\circ}$ a assinatura composta por $\Sigma^{\bullet\circ} = \{\wedge, \vee, \rightarrow, \neg, \bullet, \circ\}$. A lógica **LFI1**, $LFI1 = \langle For^{\bullet\circ}, \vdash_{LFI1}\rangle$, é axiomatizada pelo seguinte esquema de axiomas:
(Ax1) $\alpha \rightarrow (\beta \rightarrow \alpha)$;
(Ax2) $(\alpha \rightarrow \beta) \rightarrow ((\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \gamma))$;
(Ax3) $\alpha \rightarrow (\beta \rightarrow (\alpha \wedge \beta)$;
(Ax4) $(\alpha \wedge \beta) \rightarrow \alpha$;
(Ax5) $(\alpha \wedge \beta) \rightarrow \beta$;
(Ax6) $\alpha \rightarrow (\alpha \vee \beta)$;
(Ax7) $\beta \rightarrow (\alpha \vee \beta)$;
(Ax8) $(\alpha \rightarrow \gamma) \rightarrow ((\beta \rightarrow \gamma) \rightarrow ((\alpha \vee \beta) \rightarrow \gamma))$;
(Ax9) $\alpha \vee (\alpha \rightarrow \beta)$;
(Ax10) $\alpha \vee \neg\alpha$;
(Ax11) $\circ\alpha \rightarrow (\alpha \rightarrow (\neg\alpha \rightarrow \beta))$;
(Ax12) $\neg \circ \alpha \rightarrow (\alpha \wedge \neg\alpha)$;
(Ax13) $\alpha \rightarrow \neg\neg\alpha$;
(Ax14) $\neg\neg\alpha \rightarrow \alpha$;
(Ax15) $\bullet(\alpha \wedge \beta) \leftrightarrow ((\bullet\alpha \wedge \beta) \vee (\bullet\beta \wedge \alpha))$;

(Ax16) $\bullet(\alpha \vee \beta) \leftrightarrow ((\bullet\alpha \wedge \neg\beta) \vee (\bullet\beta \wedge \neg\alpha))$;
(Ax17) $\bullet(\alpha \rightarrow \beta) \leftrightarrow (\alpha \wedge \bullet\beta)$.

Regra de Inferência:
(MP): $(\alpha, \alpha \rightarrow \beta) \vdash \beta$

2.6.1 A semântica da LFI1

Em (Carnielli, Marcos & Amo 2000), os autores demonstram que a lógica paraconsistente LFI1 pode ser representada por uma matriz trivalorada, no sentido canônico, cujos valores de verdade são representados por $V = \{0, 1, 2\}$, sendo $D = \{1, 2\}$ (2 para *verdadeiro* e 1 para *parcialmente verdadeiro*), cujas matrizes de valoração são dadas por:

$\wedge$	**2**	**1**	**0**
2	**2**	**1**	**0**
1	**1**	**1**	**0**
0	**0**	**0**	**0**

$\vee$	**2**	**1**	**0**
2	**2**	**2**	**2**
1	**2**	**1**	**1**
0	**2**	**1**	**0**

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

	$\neg$	$\bullet$
2	**0**	**0**
1	**1**	**2**
0	**2**	**0**

2.6.2 O método de Polinômios para a LFI1

Definição 2.6.2. Seja $*$ uma função que traduz fórmulas LFI1 em polinômios no anel $\mathbb{Z}_3$, isto é:

$$* : For_{\{LFI1\}} \rightarrow \mathbb{Z}_3[X]$$

tal que:

$$(x \wedge y)^* = 2x^2y^2 + 2x^2y + 2xy^2 + xy;$$
$$(x \vee y)^* = x^2y^2 + x^2y + xy^2 + 2xy + x + y;$$
$$(x \rightarrow y)^* = 2x^2y^2 + x^2 + y^2 + y + 2;$$
$$(\neg x)^* = 2x + 2;$$
$$(\bullet x)^* = x^2 + x.$$

Em (Amo, Carnielli & Marcos 2002), os autores propõem uma modelagem de bancos de dados inconsistentes por meio de uma estrutura lógica paraconsistente (a LFI1). O tratamento da informação inconsistente tem aumentado consideravelmente nos últimos anos e tornou-se um importante campo de pesquisa em bancos de dados. Um sistema formal apto para manusear contradições em computação é claramente de grande interesse para a área, principalmente para aqueles que gerenciam os bancos de dados.

2.6.3 A aplicabilidade da LFI1.

Segundo (Carnielli et al. 2000), um banco de dados relacional é uma coleção finita de relações na qual a informação é armazenada. Em geral, com o intuito de se evitar dados contraditórios, as informações anexadas nesses bancos devem respeitar certas condições a fim de que as mesmas sejam inseridas de modo seguro no banco. Tais condições são conhecidas como *restrições de integridade*, e como o próprio nome sugere, essas restrições são colocadas de modo a garantir a integridade do sistema.

Tradicionalmente, quando um banco de dados é atualizado, isto é, quando uma informação é adicionada, modificada ou então removida do banco, cabe ao sistema de gerenciamento verificar se aquele conjunto de informação que foi alterado continua a satisfazer as condições de integridade, ou no caso de informação adicionada, se a integridade do sistema foi mantida. A atualização somente ocorre se, de fato, a integridade não foi prejudicada, caso contrário, o banco mantém seu estado anterior. Diante disso, em sistemas de bancos de dados tradicionais a informação contraditória nunca é permitida.

No entanto, informações inconsistentes podem ser consequências inevitáveis de algumas situações ocorridas nos bancos de dados, tal como a integração de diferentes bancos.

Com o desenvolvimento da tecnologia de rede, o acesso a informação foi potencialmente permitido e as atualizações dos diferentes sistemas que norteiam essa rede estão disponíveis para qualquer usuário. E, geralmente, quando integramos dados, esses bancos podem ser provenientes das mais diversas fontes, abrindo caminho para a possibilidade de ser ter uma inconsistência entre as informações incorporadas.

Quando um banco de dados local é desenvolvido, ele tem em sua composição interna uma série de restrições de integridade que, para aquele contexto ao qual ele foi planejado, não há qualquer indício de contradições. Porém, dois bancos de dados locais ao serem incorporados um pelo outro podem ter informações mutuamente contraditórias e, portanto, exigirem procedimentos complexos e caros para a manutenção ou a restauração da consistência global do sistema.

Além disso, segundo (Carnielli et al. 2000), uma outra característica interessante para o sistema seria que o mesmo pudesse alterar suas restrições de integridade a medida que novos bancos são integrados. Essa "evolução" nas restrições também poderia gerar informações inconsistentes, pois somos incapazes de garantir, com plena certeza, que essas novas restrições não serão contraditórias.

Vejamos um exemplo de uma integração que gera um banco de dados inconsistente. Sejam dadas as seguintes relações com as suas respectivas restrições de integridade:
$R_1 = \{R(a), Q(a), Q(b)\}$ e $C_1 = \forall x(\neg R(x) \vee Q(x))$;

$R_2 = \{R(c), Q(b)\}$ e $C_2 = \forall x(\neg R(x) \vee \neg Q(x))$;

$R_3 = \{R(b), Q(b)\}$ e $C_3 = \forall x(R(x) \vee \neg Q(x))$;

$I = R_1 \cup R_2 \cup R_3 = \{R(a), R(b), R(c), Q(a), Q(b)\}$.

Todos os bancos de dados locais, R_1, R_2 e R_3, são consistentes. No entanto, ao integrarmos

os três verificamos que as três condições acima são incompatíveis, no sentido em que elas são simultaneamente satisfeitas apenas pelo conjunto vazio.

Em recentes trabalhos, tal como em (Carnielli et al. 2007), uma família de lógicas paraconsistentes, chamadas Lógicas da Inconsistência Formal (LFIs), foram introduzidas, cuja característica principal é a internalização dos conceitos de consistência e inconsistência dentro da linguagem objeto. Neste trabalho focamos nossa atenção a uma dessas lógicas, a LFI1, a fim de usarmos essa estrutura para modelar bancos de dados integrados.

Em (Carnielli et al. 2000), constroem, a partir de um certo banco de dados integrado, uma versão reparada do mesmo, no qual informações inconsistentes podem ocorrer. O método, denominado REPAIR, é baseado no mecanismo de inferência do sistema de tablôs para a LFI. Para o caso proposicional, o REPAIR pode ser baseado em um sistema de provas por anéis de polinômios, pois as matrizes de valorações para a LFI1 proposicional são as mesmas apresentadas no início da seção.

O caso da LFI1 apenas exemplifica como lógicas multivalentes finitárias podem ser tratadas por meio de polinômios com coeficientes em corpos finitos adequados. Outros resultados podem ser encontrados em (Carnielli et al. 2007). Nosso tratamento original para a os sistemas verificados nessa seção, em sua versão polinomial, apenas complementa o quadro no que diz respeito às LFIs.

Capítulo 3

Semânticas não-determinísticas em uma versão polinômica

"Never ask for the meaning of a word in isolation, but only in the context of a sentence".
(Gottlob Frege em *Grundlagen der Arithmetik*).

Em uma série de artigos tais como (Avron & Konikowska 2005), (Avron & Levi 2005), (Avron 2007) e (Avron 2008), Arnon Avron representa uma boa parte das LFI's em forma de matrizes não-determiníticas - Nmatrizes. O foco deste capítulo, representando nosso esforço original, está na aplicabilidade no método de anéis de polinômios em sistemas lógicos cujas semânticas são não-determinísticas.

3.1 As N-matrizes de Arnon Avron

O princípio da *Verofuncionalidade* (ou *Composicionalidade*) é um princípio geral na constituição semântica de diversos sistemas lógicos (clássicos e não-clássicos) que afirma que o valor-verdade de sentenças complexas deve ser determinado em função dos valores-verdade de suas subsentenças. Nas palavras de Janssen, em (Janssen 2001), p. 115.

"The meaning of a compound expression is a function of the meaning of its parts and of the syntactic rule by which they are combined".

No caso específico da lógica clássica, sua linguagem completa contém uma coleção de conectivos m-ários que constroem fórmulas complexas, sendo as mesmas caracterizadas por tabelas de verdade com, no mínimo, 2^m linhas, sendo que cada uma dessas linhas representa um possível valor de verdade atribuído as suas componentes sentenciais. Assim, a tabela de verdade para um conectivo binário $\sharp$ pode ser visto como apresentado na figura abaixo, onde cada $p_{i,j}$ representa um valor de verdade em $\{0, 1\}$. Logo:

$\sharp$	0	1
0	$p_{0,0}$	$p_{0,1}$
1	$p_{1,0}$	$p_{1,1}$

Uma generalização das tabelas de verdade, para um número arbitrário de valores de verdade, está na construção de lógicas multivaloradas contendo "*graus de falsidade*"e "*graus de verdade*", ao invés da bivaloração, conforme discutido por João Marcos em (Marcos 2009). Diante disso, o conjunto de valores de verdade pode ser qualquer coleção $\{0, ..., x, y, ..., 1\}$, no qual os valores ditos *não-distinguidos*,$\{0, ..., x\}$ permitem graus de falsidade e os valores ditos *distinguidos*, $\{y, ..., 1\}$, permitem graus de verdade. Neste caso, a tabela de verdade de um conectivo binário $\sharp$ seria da seguinte forma:

$\sharp$	0	...	x	y	...	1
0	$p_{0,0}$	$\vdots$	$p_{0,x}$	$p_{0,y}$	$\vdots$	$p_{0,1}$
$\vdots$	$\vdots$	$\ddots$	...	...	$\ddots$	$\vdots$
x	$p_{x,0}$	$\vdots$	$p_{x,x}$	$p_{x,y}$	$\vdots$	$p_{x,1}$
y	$p_{y,0}$	$\vdots$	$p_{y,x}$	$p_{y,y}$	$\vdots$	$p_{y,1}$
$\vdots$	$\vdots$	$\ddots$	...	...	$\ddots$	$\vdots$
1	$p_{1,0}$	$\vdots$	$p_{1,x}$	$p_{1,y}$	$\vdots$	$p_{1,1}$

No entanto, há um cenário muito mais fundamental, no qual se pode generalizar o conceito de uma estrutura multivalorada, em que a atribuição de verdade de uma fórmula complexa qualquer seja escolhida de modo não-determinístico a partir de um certo conjunto não-vazio de opções. Arnon Avron denominou essas estruturas por *Matrizes Não-Determinísticas*, ou *NMatrizes*. Contudo, a concepção de matrizes não determinísticas já havia sido exposta por Quine em sua obra *The Roots of Reference.*[1]

Em *The Roots of Reference*, Quine esboça uma teoria disposicional do que ele chamou de *significado primitivo* dos operadores lógicos e observa que essa semântica falha na verofuncionalidade.

Para Quine uma sentença é dita *analítica* quando sua verdade é apreendida por meio do aprendizado de suas palavras. Como um caso particular, aprendemos o significado das palavras lógicas encontrando conexões disposicionais.

Em se tratando do operador clássico da negação, podemos inferir que: aprendemos a concordar com $\neg A$ (respectivamente discordar) exatamente quando discordamos de A (respectivamente concordamos). No entanto, para os operadores da conjunção e disjunção, a situação não é tão simples assim.

Quine diz que uma conjunção estabelece a concordância quando, e apenas quando, cada um dos seus componentes também estabelece a concordância. No caso da discordância, temos que a conjunção estabelece a discordância sempre que um dos seus componentes discorda. Porém, segundo Quine, há um ponto cego em relação à conjunção, que ocorre quando nenhum componente estabelece concordância ou discordância. Não há uma maneira direta de resolver este ponto cego. Em alguns casos a conjunção estabelece discordância e em outros nada é estabelecido, conforme apresentado na tabela abaixo.

[1]Agradecemos ao Prof. Marcello D'Agostino, da Universidade de Ferrara, pela sugestão de que as Nmatrizes já haviam sido pensadas e formuladas por Quine (comunicação pessoal).

$p \wedge q$	c	a	d
c	c	a	d
a	a	?	d
d	d	d	d

$p \vee q$	c	a	d
c	c	a	d
a	c	?	a
d	c	a	d

Onde, a denota abstém, c significa concorda e d, discorda.

Na visão de Quine, os operadores de conjunção e disjunção que emergem essas tabelas trivaloradas com valores incompletos são mais primitivos do que as tabelas-verdade usuais de conjunção e disjunção, na medida em que eles podem ser aprendidas por indução a partir da observação do "comportamento veriditivo", (Quine 1973), p. 78. Além disso, tais tabelas são independentes da nossa lógica de dois valores, e independente de outras lógicas verofuncionais. Isso significa que a verofuncionalidade, tida como básica em lógica e vista por alguns como sacrossanta, não passa de um caso limite, simples mas não essencial (veja a discussao na seção 1 desse capítulo). Nosso tratamento via polinômios consegue dar uma roupagem algébrica a essa intuição transformando-a num objeto matemático concreto.

Em "Non-deterministic Semantics for Logical Systems", (Avron 2007), Arnon Avron propõe uma solução para o problema da explicitação da verofuncionalidade em certos sistemas lógicos por meio de um relaxamento do princípio em si. O autor defende a ideia de computações não-determinísticas dos valores de verdade, através de uma generalização das conhecidas matrizes multivaloradas, em que o valor de verdade de uma determinada fórmula complexa é escolhido não-deterministicamente dentro de um conjunto de opções.

Há algumas motivações para a introdução do não-determinismo ou indeterminismo dentro das tabelas de verdade dos conectivos lógicos. Destacamos, conforme (Avron & Zamansky 2011), as seguintes:

(i) *Subespecificação Sintática.*

Consideremos a semântica clássica correspondente ao conjunto completo de conectivos, $\{\neg, \vee\}$ com suas respectivas tabelas de verdade:

	$\neg$
t	f
f	t

		$\vee$
t	t	t
t	f	t
f	t	t
f	f	f

Suponhamos, neste momento, que o Princípio do Terceiro excluído seja rejeitado, no espírito da lógica intuicionaista, ou seja, há situações em que $A \vee \neg A$ nem sempre é verdadeira.Um exemplo muito utilizado para expressar tal situação é a Conjectura de Goldbach, segundo a qual todo número inteiro par maior que 2 é igual à soma de dois primos.

Apesar de verificarmos, um a um, até onde pudermos ir, que sempre encontramos os dois primos, não é possível provar a conjectura percorrendo todo o conjunto dos números naturais e testando todos esses números. Sendo assim, até hoje não foi encontrada uma prova de que a Conjectura de Goldbach, denotada a partir de agora por **G**, seja verdadeira e nem um contra-exemplo para demonstrar a sua falsidade. Em resumo, não há uma prova de **G** e nem de $\neg\mathbf{G}$. Assim, neste caso, não podemos afirmar que $\mathbf{G} \vee \neg\mathbf{G}$ é uma proposição verdadeira, segundo os intuicionistas.

Mas, como seria a semântica do sistema com tal modificação? Intuitivamente, a não admissão deste Princípio do Terceiro Excluído acarreta em uma perda da informação a respeito da segunda linha da tabela de verdade para a negação, ou seja, se o valor de verdade de uma sentença φ é falso quando φ ainda não foi demonstrada, então a negação de φ pode ser tanto verdadeira quanto falsa . Por outro lado, tomando φ como verdadeira, se φ foi demonstrado então $\neg\varphi$ é certamente falso (admitindo a consistência clássica da lógica). Diante disso, ficamos com um problema de *subespecificação*, no qual todos os possíveis valores de verdade são permitidos.

A semântica adequada a este caso é a de Nmatrizes, tal como:

	$\widetilde{\neg}$
t	$\{f\}$
f	$\{t, f\}$

		$\widetilde{\vee}$
t	t	$\{t\}$
t	f	$\{t\}$
f	t	$\{t\}$
f	f	$\{f\}$

(ii) *Ambiguidade linguística.*

Na maioria das linguagens naturais, a palavra **ou** pode ter dois sentidos: um inclusivo e outro exclusivo. Por exemplo, consideremos as seguintes sentenças:
i) "O seguro será pago em caso de incêndio ou roubo".
ii) "Esta noite, as 20h00, estarei em um ônibus ou em um avião, rumo à Argentina".

No primeiro caso, (i), o significado do vocábulo **ou** é inclusivo enquanto que em (ii) é exclusivo. O problema inerente a estas distinções decorre do fato que, em muitos casos, não conseguimos distinguir essa diferença quando um interlocutor pronuncia uma sentença com o conectivo **ou**. No entanto, mesmo nestes casos gostaríamos de realizar inferências a partir daquilo que nos foi dito e, de fato, isto pode ser capturado pelas Nmatrizes conforme explicitado abaixo, notando que $t \vee t$ terá valor f se "ou"tiver um sentido exclusivo e t, caso contrário.

		$\vee$
t	t	$\{t, f\}$
t	f	$\{t\}$
f	t	$\{t\}$
f	f	$\{f\}$

(iii) *Comportamento não-determinístico inerente aos circuitos.*

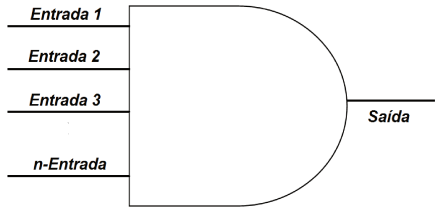
As Nmatrizes podem ser aplicadas para modelar comportamentos não-determinísticos de circuitos elétricos. Uma porta lógica ideal que realiza operações em variáveis booleanas é uma abstração de uma porta operacional física com uma variedade contínua de quantidade elétrica,

sendo que esta quantidade elétrica é tranformada em uma variável discreta, associando todo um domínio de tensões elétricas aos valores lógicos 1 e 0.

Os circuitos eletrônicos, ou de lógica digital, tratam do estudo e comportamento dos dispositivos eletrônicos de dois estados, enfatizando as relações existentes entre esses estados. Há, portanto, dois estados lógicos a serem considerados neste caso:

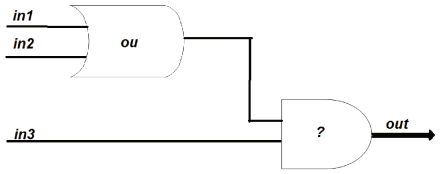
- 0**(zero)**: É o estado lógico que representa, por exemplo, porta fechada, aparelho desligado, ausência de tensão, chave aberta, etc.
- 1**(um)**: É o estado lógico que representa, por exemplo, porta aberta, aparelho ligado, presença de tensão, chave fechada, etc.

As portas lógicas são circuitos eletrônicos que a partir de um um conjunto de sinais lógicos produzem um sinal de saída, ou seja:



Muitos fatores podem alterar o comportamento esperado de um circuito como a presença de fontes perturbadoras de ruídos, temperaturas, mal contato, roubo de energia, etc. A exata matemática da relação entre entrada e saída de uma dada porta lógica nem sempre é conhecida e podemos representar tal fato por uma tabela de verdade não-determinística.

Por exemplo, suponhamos o seguinte circuito formado por uma porta padrão *OR* e uma porta defeituosa *AND*, a qual responde corretamente se as entradas forem similares e imprevisivelmente caso contrário.



O comportamento da porta *AND* defeituosa pode ser descrito pela seguinte Nmatriz:

		$\wedge$
t	t	$\{t\}$
t	f	$\{t, f\}$
f	t	$\{t, f\}$
f	f	$\{f\}$

3.2 O conceito de uma matriz Não-Determinística

As Nmatrizes foram introduzidas por Arnon Avron nos seguintes artigos: (Avron & Levi 2005), (Avron & Konikowska 2005),(Avron 2008). As definições que apresentaremos abaixo foram extraídas desses trabalhos.

Definição 3.2.1. Uma *Matriz Não-determinística* (*Nmatriz*) para uma linguagem proposicional $\mathcal{L}$ é uma tripla $\mathcal{M} = \langle \mathcal{V}, \mathcal{D}, \mathcal{O} \rangle$, onde:

- $\mathcal{V}$ é um conjunto não-vazio de *valores de verdade*;
- $\mathcal{D}$ é um subconjunto não-vazio, próprio, de $\mathcal{V}$, ou seja, $\mathcal{D} \subseteq \mathcal{V}$.
- Para todo conectivo n-ário $\diamond$ de $\mathcal{L}$, $\mathcal{O}$ contém uma correspondente função n-ária $\widetilde{\diamond}$ de $\mathcal{V}^n$ em $2^{\mathcal{V}} - \{\emptyset\}$.

Dizemos que $\mathcal{M}$ é *(in)finita* se $\mathcal{V}$ também é (in)finito.

Definição 3.2.2. Consideremos W como um conjunto de fórmulas de $\mathcal{L}$. Uma valoração (legal) em um Nmatriz $\mathcal{M}$ é uma função $v : W \to \mathcal{V}$ que satisfaz as seguintes condições para qualquer conectivo n-ário $\diamond$ de $\mathcal{L}$ e $\psi_1, ..., \psi_n \in W$:

$$v(\diamond(\psi_1, ..., \psi_n)) \in \widetilde{\diamond}(v(\psi_1), ..., v(\psi_n)).$$

Definição 3.2.3. Uma valoração v em uma Nmatriz $\mathcal{M}$ é um *modelo* de (ou satisfaz) uma fórmula em $\mathcal{M}$ (notação:$v \models_{\mathcal{M}} \mathbf{T}$) se $v(\psi) \in \mathcal{D}$. v é um modelo em $\mathcal{M}$ de um conjunto $\mathbf{T}$ de fórmulas se ele satisfaz todas as fórmulas de $\mathbf{T}$.

Definição 3.2.4. A relação de consequência induzida pela Nmatriz $\mathcal{M}$ (Notação: $\vdash_{\mathcal{M}}$) é definida por:

$$\mathbf{T} \vdash_{\mathcal{M}} \varphi \text{ se para toda valoração } v \text{ tal que } v \models_{\mathcal{M}} \mathbf{T}, \text{ também } v \models_{\mathcal{M}} \varphi.$$

Definição 3.2.5. Uma lógica $\mathbf{L} = \langle \mathcal{L}, \vdash_{\mathbf{L}} \rangle$ é dita *correta* para uma Nmatriz $\mathcal{M}$ (onde $\mathcal{L}$ é a linguagem de $\mathcal{M}$) se $\vdash_{\mathbf{L}} \subseteq \vdash_{\mathcal{M}}$.
(i) $\mathcal{M}$ é a característica para $\mathbf{L}$ se $\mathbf{L}$ é correta e completa para $\mathcal{M}$, isto é: $\vdash_{\mathbf{L}} = \vdash_{\mathcal{M}}$.
(ii) $\mathcal{M}$ é fracamente característica para $\mathbf{L}$ se, para toda fórmula φ de $\mathcal{L}$, $\vdash_{\mathbf{L}} \varphi$ se e somente se $\vdash_{\mathcal{M}} \varphi$.

Observação 3.2.6. Identificaremos como uma matriz determinística as Nmatrizes cujas funções retornam, sempre, valores unitários em $2^{\mathcal{V}} - \{\emptyset\}$.

Exemplo 3.2.7. Consideremos a linguagem $\mathcal{L} = \langle \wedge, \vee, \rightarrow, \neg \rangle$, cujos operadores $(\wedge, \vee, \rightarrow)$ são interpretados classicamente e a negação permite a lei da contradição mas não aceita, necessariamente, a lei do terceiro excluído. Estas condições nos levam às seguintes Nmatrizes $\mathcal{M}^2 = (\mathcal{V}, \mathcal{D}, \mathcal{O})$ para $\mathcal{L}$, onde $\mathcal{V} = \{t, f\}$, $\mathcal{D} = \{t\}$ e $\mathcal{O}$ é dada por:

	$\widetilde{\neg}$
t	$\{f\}$
f	$\{t, f\}$

		$\widetilde{\vee}$	$\widetilde{\wedge}$	$\widetilde{\rightarrow}$
t	t	$\{t\}$	$\{t\}$	$\{t\}$
t	f	$\{t\}$	$\{f\}$	$\{f\}$
f	t	$\{t\}$	$\{f\}$	$\{t\}$
f	f	$\{f\}$	$\{f\}$	$\{t\}$

Notemos que a negação clássica pode ser definida em $\mathcal{M}^2$ por: $\sim \psi = \psi \rightarrow \neg\psi$. Em termos de tabela de verdade temos:

ψ	$\neg\psi$	$\rightarrow$
t	$\{f\}$	$\{f\}$
f	$\{t, f\}$	$\{t\}$

Exemplo 3.2.8. Consideremos as seguintes Nmatrizes trivaloradas $\mathcal{M}^3_{\mathbf{L}}$ e $\mathcal{M}^3_{\mathbf{S}}$. As interpretações para a disjunção, conjunção e implicação são as mesmas para $\mathcal{M}^3_{\mathbf{L}}$ e $\mathcal{M}^3_{\mathbf{S}}$ e corresponde à interpretação tradicional clássica. A diferença entre estas Nmatrizes está no operador da negação, sendo este mais geral em $\mathcal{M}^3_{\mathbf{L}}$ e mais específico em $\mathcal{M}^3_{\mathbf{S}}$. Apenas para uma questão de notação, o símbolo | representará a palavra *ou*. Assim, temos:

$$a\widetilde{\vee}b = \begin{cases} \mathcal{D}, & a \in \mathcal{D} \mid b \in \mathcal{D} \\ \mathcal{F}, & a, b \in \mathcal{F} \end{cases} \tag{3.1}$$

$$a\widetilde{\wedge}b = \begin{cases} \mathcal{F}, & a \in \mathcal{F} \mid b \in \mathcal{F} \\ \mathcal{D}, & a, b \in \mathcal{D} \end{cases} \tag{3.2}$$

$$a\widetilde{\rightarrow}b = \begin{cases} \mathcal{D}, & a \in \mathcal{F} \mid b \in \mathcal{D} \\ \mathcal{F}, & a \in \mathcal{D}, b \in \mathcal{F} \end{cases} \tag{3.3}$$

	$\widetilde{\neg}_{\mathcal{M}^3_{\mathbf{L}}}$
t	$\{f\}$
$\top$	$\mathcal{V}$
f	$\{t\}$

	$\widetilde{\neg}_{\mathcal{M}^3_{\mathbf{S}}}$
t	$\{f\}$
$\top$	$\mathcal{D}$
f	$\{t\}$

3.2.1 Alguns sistemas lógicos com Nmatrizes finito-valoradas

Apresentaremos alguns sistemas finito-valorados com Nmatrizes a fim de os utilizarmos para a tradução em polinômios.

1. **O sistema mbC.**

Uma Nmatriz para mbC, em uma linguagem $\mathcal{L} = \{\wedge, \vee, \rightarrow, \neg, \circ\}$ é definida por:

- $\mathcal{V} = \{\mathcal{T} \biguplus \mathcal{I} \biguplus \mathcal{F}\}$, onde $\mathcal{T}$, $\mathcal{I}$, e $\mathcal{F}$ são conjuntos não-vazios e dois a dois disjuntos, tais que: $\mathcal{T} = \{t\}$, $\mathcal{F} = \{f\}$ e $\mathcal{I} = \{I\}$
- $\mathcal{D} = \mathcal{T} \cup \mathcal{I}$
- $\mathcal{O}$ é definida por:

$$a\widetilde{\vee}b = \begin{cases} \mathcal{D}, & a \in \mathcal{D} \mid b \in \mathcal{D} \\ \mathcal{F}, & a, b \in \mathcal{F} \end{cases} \tag{3.4}$$

$$a\widetilde{\wedge}b = \begin{cases} \mathcal{F}, & a \in \mathcal{F} \mid b \in \mathcal{F} \\ \mathcal{D}, & a, b \in \mathcal{D} \end{cases} \tag{3.5}$$

$$a\widetilde{\rightarrow}b = \begin{cases} \mathcal{D}, & a \in \mathcal{F} \mid b \in \mathcal{D} \\ \mathcal{F}, & a \in \mathcal{D}, b \in \mathcal{F} \end{cases} \tag{3.6}$$

$$\widetilde{\neg}a = \begin{cases} \mathcal{F}, & a \in \mathcal{T} \\ \mathcal{D}, & c.c \end{cases} \tag{3.7}$$

$$\widetilde{\circ}a = \begin{cases} \mathcal{V}, & a \in (\mathcal{F} \cup \mathcal{T}) \\ \mathcal{F}, & a \in \mathcal{I} \end{cases} \tag{3.8}$$

Em termos de tabelas de verdade, as tabelas não-determinísticas referentes aos operadores definidos acima são as seguintes[2]:

$\widetilde{\vee}$	f	I	t
f	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$
I	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
t	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$

$\widetilde{\vee}$	f	I	t
f	$\{f\}$	$\{t, I\}$	$\{t, I\}$
I	$\{t, I\}$	$\{t, I\}$	$\{t, I\}$
t	$\{t, I\}$	$\{t, I\}$	$\{t, I\}$

$\widetilde{\wedge}$	f	I	t
f	$\{f\}$	$\{f\}$	$\{f\}$
I	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$
t	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$

$\widetilde{\wedge}$	f	I	t
f	$\{f\}$	$\{f\}$	$\{f\}$
I	$\{f\}$	$\{t, I\}$	$\{t, I\}$
t	$\{f\}$	$\{t, I\}$	$\{t, I\}$

$\widetilde{\rightarrow}$	f	I	t
f	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
I	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$
t	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$

[2]Com a finalidade de facilitar a leitura das tabelas para as Nmatrizes, as escreveremos de duas formas: uma com a representação do conjunto $\mathcal{D}$ e outra explicitando os próprios elementos de $\mathcal{D}$, isto é, $\mathcal{D} = \{t, I\}$

$\widetilde{\rightarrow}$	f	I	t
f	$\{t, I\}$	$\{t, I\}$	$\{t, I\}$
I	$\{f\}$	$\{t, I\}$	$\{t, I\}$
t	$\{f\}$	$\{t, I\}$	$\{t, I\}$

$\widetilde{\neg}$	f	I	t
	$\mathcal{D}$	$\mathcal{D}$	$\{f\}$

$\widetilde{\neg}$	f	I	t
	$\{t, I\}$	$\{t, I\}$	$\{f\}$

$\widetilde{\circ}$	f	I	t
	$\mathcal{D}$	$\{f\}$	$\mathcal{D}$

$\widetilde{\circ}$	f	I	t
	$\{t, I\}$	$\{f\}$	$\{t, I\}$

2. **O sistema mCi.**

A semântica em uma Nmatriz para a lógica paraconsistente mCi é constituída por 5 valores de verdade, sendo eles: $\{T, F, t, f, I\}$. Intuitivamente, I é o valor de verdade das proposições inconsistentes, T e F são os valores de verdade de proposições que são *necessariamente* consistentes, enquanto t e f são os valores de verdade para proposições *contingentemente* consistentes.

Definição 3.2.9. Uma Nmatriz para a lógica mCi, em uma linguagem $\mathcal{L} = \{\wedge, \vee, \rightarrow, \neg, \circ\}$ é composta por $\mathcal{M}_{mCi} = \langle \mathcal{V}, \mathcal{D}, \mathcal{O} \rangle$ onde:

- $\mathcal{V} = \{I, T, F, t, f\}$.
- $\mathcal{D} = \{I, T, t\}$
- $\mathcal{O}$ é definida por:

$$a\widetilde{\vee}b = \begin{cases} \{t, I\}, & a \in \mathcal{D} \mid b \in \mathcal{D} \\ \{f\}, & a, b \notin \mathcal{D} \end{cases} \tag{3.9}$$

$$a\widetilde{\wedge}b = \begin{cases} \{f\}, & a \notin \mathcal{D} \mid b \notin \mathcal{D} \\ \{t, I\}, & a \in \mathcal{D}, b \in \mathcal{D} \end{cases} \tag{3.10}$$

$$a\widetilde{\rightarrow}b = \begin{cases} \{t, I\}, & a \notin \mathcal{D} \mid b \in \mathcal{D} \\ \{f\}, & a \in \mathcal{D}, b \notin \mathcal{D} \end{cases} \tag{3.11}$$

$$\widetilde{\neg}a = \begin{cases} \{F\}, & a = T \\ \{T\}, & a = F \\ \{f\}, & a = t \\ \{t, I\}, & a \in \{f, I\} \end{cases} \tag{3.12}$$

$$\widetilde{\circ}a = \begin{cases} \{F\}, & a = I \\ \{T\}, & a \neq I \end{cases} \tag{3.13}$$

Em termos de tabelas de verdade, as tabelas não-determinísticas referentes aos operadores definidos acima são as seguintes:

$\widetilde{\vee}$	f	F	I	t	T
f	$\{f\}$	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
F	$\{f\}$	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
I	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
t	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
T	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$

$\widetilde{\vee}$	f	F	I	t	T
f	$\{f\}$	$\{f\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$
F	$\{f\}$	$\{f\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$
I	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$
t	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$
T	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$

$\widetilde{\wedge}$	f	F	I	t	T
f	$\{f\}$	$\{f\}$	$\{f\}$	$\{f\}$	$\{f\}$
F	$\{f\}$	$\{f\}$	$\{f\}$	$\{f\}$	$\{f\}$
I	$\{f\}$	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
t	$\{f\}$	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
T	$\{f\}$	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$

$\widetilde{\wedge}$	f	F	I	t	T
f	$\{f\}$	$\{f\}$	$\{f\}$	$\{f\}$	$\{f\}$
F	$\{f\}$	$\{f\}$	$\{f\}$	$\{f\}$	$\{f\}$
I	$\{f\}$	$\{f\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$
t	$\{f\}$	$\{f\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$
T	$\{f\}$	$\{f\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$

$\widetilde{\rightarrow}$	f	F	I	t	T
f	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
F	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
I	$\{f\}$	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
t	$\{f\}$	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
T	$\{f\}$	$\{f\}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$

$\widetilde{\rightarrow}$	f	F	I	t	T
f	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$
F	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$
I	$\{f\}$	$\{f\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$
t	$\{f\}$	$\{f\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$
T	$\{f\}$	$\{f\}$	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$

$\widetilde{\neg}$	f	F	I	t	T
	$\mathcal{D}$	$\{T\}$	$\mathcal{D}$	$\{f\}$	$\{F\}$

$\widetilde{\neg}$	f	F	I	t	T
	$\{I,t\}$	$\{T\}$	$\{I,t\}$	$\{f\}$	$\{F\}$

$\widetilde{\circ}$	f	F	I	t	T
	$\{T\}$	$\{T\}$	$\{F\}$	$\{T\}$	$\{T\}$

Os teoremas de correção e completude desse sistema são apresentados em (Avron 2007).

3. **Outros sistemas paraconsistentes**.

Em seu paper "Non-deterministic Semantics for Logics with a Consistency Operator", (Avron 2007), Arnon Avron apresenta de um modo sucinto e simples as Nmatrizes para 64 das principais LFIs apresentadas por (Carnielli et al. 2007). Esboçaremos aqui apenas algumas delas.

É importante salientarmos que os teoremas de correção e completude, para todos os sistemas em questão, são demonstrados neste trabalho de Avron.

Definição 3.2.10. Seja Ax o conjunto formado pelos seguintes axiomas:
(c) $\neg\neg\varphi \rightarrow \varphi$
(e) $\varphi \rightarrow \neg\neg\varphi$
(i) $\neg \circ \varphi \rightarrow (\varphi \wedge \neg\varphi)$
(a) $(\circ\varphi \wedge \circ\psi) \rightarrow (\circ(\varphi \wedge \psi) \wedge \circ(\varphi \vee \psi) \wedge \circ(\varphi \rightarrow \psi))$
(o) $(\circ\varphi \vee \circ\psi) \rightarrow (\circ(\varphi \wedge \psi) \wedge \circ(\varphi \vee \psi) \wedge \circ(\varphi \rightarrow \psi))$
(l) $\neg(\varphi \wedge \neg\varphi) \rightarrow \circ\varphi$
(d) $\neg(\neg\varphi \wedge \varphi) \rightarrow \circ\varphi$
(b) $(\neg(\varphi \wedge \neg\varphi) \vee (\neg(\neg\varphi \wedge \varphi)) \rightarrow \circ\varphi$

Para $X \subseteq Ax$, **mbC[X]** é o sistema obtido de mbC pela adição de alguns dos axiomas de Ax.

Notação 3.2.11. Para facilidade de notação, utilizaremos **mbCs** ao invés de **mbC[X]** a fim de explicitarmos o sistema formado por mbC mais s axiomas do conjunto Ax, como por exemplo em **mbCiel** o qual representa mbC munida dos axiomas (i), (e) e (l).

Definição 3.2.12. As condições em mbC-Nmatrizes que correspondem aos axiomas (i), (c), (e), (a) e (o) são as seguintes:
Cond(i): $a \in \mathcal{T} \cup \mathcal{F} \Rightarrow \widetilde{\circ}a \subseteq \mathcal{T}$.
Cond(c): $a \in \mathcal{F} \Rightarrow \widetilde{\neg}a \subseteq \mathcal{T}$.
Cond(e): $a \in \mathcal{I} \Rightarrow \widetilde{\neg}a \subseteq \mathcal{I}$.
Cond(a): $a \in \mathcal{T} \cup \mathcal{F}$ e $b \in \mathcal{T} \cup \mathcal{F} \Rightarrow a\widetilde{\sharp}b \subseteq \mathcal{T} \cup \mathcal{F}, (\sharp \in \{\vee, \wedge, \rightarrow\})$.
Cond(o): $a \in \mathcal{T} \cup \mathcal{F}$ ou $b \in \mathcal{T} \cup \mathcal{F} \Rightarrow a\widetilde{\sharp}b \subseteq \mathcal{T} \cup \mathcal{F}, (\sharp \in \{\vee, \wedge, \rightarrow\})$.

Definição 3.2.13. Seja $\mathcal{S} = \{i, c, e, ci, ie, ce, cie, ia, cia, iae, ciae, io, cio, ioe, cioe\}$.

- Para $s \in \mathcal{S}$, uma mbCs-Nmatriz é uma mbC-Nmatriz que satisfaz a *Cond(x)* para todo x que ocorre em s.
- $\mathcal{M}_{mbCs}$ é a única mbCs-Nmatriz em que $\mathcal{T} = \{t\}$, $\mathcal{F} = \{f\}$ e $\mathcal{I} = \{I\}$

As tabelas de verdade para as mbCs-Nmatrizes são definidas por:

1. Se o axioma (i) ocorre em s, então a tabela de verdade de $\mathcal{M}_{mbCs}$ correspondente ao conectivo $\circ$ é dada por:

$\widetilde{\circ}$	f	I	t
	$\{t\}$	$\{f\}$	$\{t\}$

2. Em $\mathcal{M}_{mbCc}$, $\mathcal{M}_{mbCci}$, $\mathcal{M}_{mbCcia}$ e $\mathcal{M}_{mbCcio}$ a tabela de verdade correspondente ao conectivo $\neg$ é dada por:

$\widetilde{\neg}$	f	I	t
	$\{t\}$	$\{I,t\}$	$\{f\}$

3. Em $\mathcal{M}_{mbCe}$, $\mathcal{M}_{mbCie}$, $\mathcal{M}_{mbCiae}$ e $\mathcal{M}_{mbCioe}$ a tabela de verdade correspondente ao conectivo $\neg$ é dada por:

$\widetilde{\neg}$	f	I	t
	$\{I,t\}$	$\{I\}$	$\{f\}$

4. Em $\mathcal{M}_{mbCce}$, $\mathcal{M}_{mbCcie}$, $\mathcal{M}_{mbCciae}$ e $\mathcal{M}_{mbCcioe}$ a tabela de verdade correspondente ao conectivo $\neg$ é dada por:

$\widetilde{\neg}$	f	I	t
	$\{t\}$	$\{I\}$	$\{f\}$

5. Se **a** ocorre em s, então a tabela de verdade de $\mathcal{M}_{mbCs}$ correspondente aos conectivos $\{\vee, \wedge, \rightarrow\}$ é dada por:

$\widetilde{\vee}$	f	I	t
f	$\{f\}$	$\{I,t\}$	$\{t\}$
I	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$
t	$\{t\}$	$\{I,t\}$	$\{t\}$

$\widetilde{\wedge}$	f	I	t
f	$\{f\}$	$\{f\}$	$\{f\}$
I	$\{f\}$	$\{I,t\}$	$\{I,t\}$
t	$\{f\}$	$\{I,t\}$	$\{t\}$

$\widetilde{\rightarrow}$	f	I	t
f	$\{t\}$	$\{I,t\}$	$\{t\}$
I	$\{f\}$	$\{I,t\}$	$\{I,t\}$
t	$\{f\}$	$\{I,t\}$	$\{t\}$

6. Se **o** ocorre em s, então a tabela de verdade de $\mathcal{M}_{mbCs}$ correspondente aos conectivos $\{\vee, \wedge, \rightarrow\}$ é dada por:

$\widetilde{\vee}$	f	I	t
f	$\{f\}$	$\{t\}$	$\{t\}$
I	$\{t\}$	$\{I,t\}$	$\{t\}$
t	$\{t\}$	$\{t\}$	$\{t\}$

$\widetilde{\wedge}$	f	I	t
f	$\{f\}$	$\{f\}$	$\{f\}$
I	$\{f\}$	$\{I,t\}$	$\{t\}$
t	$\{f\}$	$\{t\}$	$\{t\}$

$\widetilde{\rightarrow}$	f	I	t
f	$\{t\}$	$\{t\}$	$\{t\}$
I	$\{f\}$	$\{I,t\}$	$\{t\}$
t	$\{f\}$	$\{t\}$	$\{t\}$

3.3 As Nmatrizes e o método de Provas de Anéis de Polinômios

Durante muito tempo houve uma lacuna em uma das classes mais importante e útil das LFIs, a dos *Sistemas C*. Tal lacuna centrava-se no fato de que não possuíamos uma semântica intuitiva para trabalharmos nesses sistemas. Tal problema foi sanado, segundo Avron em (Avron 2008), com a implementação das semânticas não-determinísticas, as quais oferecem uma visão real sobre esses sistemas. No entanto, esta observação é exagerada, pois as matrizes não-determinísticas de Avron são casos particulares das Semânticas de Traduções Possíveis, conferir (Carnielli 2000).

É importante salientarmos aqui que, apesar de ser algo notório, as Nmatrizes são particularmente úteis para o raciocínio sobre a incerteza já que, a incerteza sobre o valor de verdade atribuído a uma determinada fórmula é expressa na construção das suas tabelas de verdade. Além disso, a semântica das Nmatrizes finitas é decidível e portanto, a lógica constituída por tal semântica é decidível.

Nosso objetivo neste momento é traduzir as Nmatrizes de Avron em termos de anéis de polinômios.

3.3.1 O método geral de obtenção dos polinômios para as Nmatrizes.

Conforme apresentado nas seções anteriores, uma N-matriz para uma lógica específica $\mathcal{L}$ é definida pela tripla $\mathcal{M} = \langle \mathcal{V}, \mathcal{D}, \mathcal{O} \rangle$, em que $\mathcal{V}$ é um conjunto de valores de verdade, $\mathcal{D}$ é um conjunto de valores de verdade distinguidos e $\mathcal{O}$ é um conjunto que contém uma correspondente função n-ária, do conjunto de valores de verdade no conjunto das partes desse mesmo conjunto (menos o vazio), para cada um dos conectivos n-ários de $\mathcal{L}$.

O procedimento de obtenção dos anéis de polinômios para uma lógica não-determinística $\mathcal{L}$ pode ser descrito pelos seguintes passos:

1. O primeiro passo consiste em tornar uma matriz n-valorada e não-determinística em determinística e bivalorada. Para tanto, nos espaços da matriz onde houver mais de um valor de verdade, os substituiremos pelo valor 1[3].

2. Para cada operador, a partir do polinômio geral para um sistema n-valorado, aplicamos ponto a ponto as combinações bivalentes dos valores de verdade (quando os operadores forem bivalentes) ou então os valores unários para operadores unários, determinando assim um sistema linear e resolvendo como no caso clássico.

3. Ao término da resolução do sistema, encontraremos o polinômio parcial do operador em análise.

4. Por fim, analisa-se os valores das Nmatrizes em função das variáveis ocultas.

Suponhamos, por exemplo, que nossa Nmatriz seja constituída por $\mathcal{M} = \langle \mathcal{V}, \mathcal{D}, \mathcal{O} \rangle$, em que:

- $\mathcal{V} = \{0, 1, 2\}$;

[3]Esse passo pode ser realizado de outro modo, conforme veremos mais adiante.

- $\mathcal{D} = \{1, 2\}$;
- $\mathcal{O}$ é uma operação definida, matricialmente, por:

$\widetilde{\otimes}$	0	2	1
0	$\{0\}$	$\{1,2\}$	$\{1,2\}$
2	$\{1,2\}$	$\{1,2\}$	$\{1,2\}$
1	$\{1,2\}$	$\{1,2\}$	$\{1,2\}$

Como a o sistema é trivalorado e o operador é binário, o polinômio geral que utilizaremos é dado por:
(i)$p(x, y) = ax^2y^2 + a'x^2y + a''x^2y^0 + bxy^2 + b'xy + b''xy^0 + cx^0y^2 + c'x^0y + c''x^0y^0$.

Passo 1: Substituir os espaços da Nmatriz com mais de uma valor de verdade pelo valor 1. Assim, temos:

$\widetilde{\otimes}$	0	2	1
0	$\{0\}$	$\{1\}$	$\{1\}$
2	$\{1\}$	$\{1\}$	$\{1\}$
1	$\{1\}$	$\{1\}$	$\{1\}$

Passo 2: Resolver o sistema proveniente das substituições dos pares de valores de verdade, e seus respectivos resultados, no polinômio geral:

$$p(x, y) = ax^2y^2 + a'x^2y + a''x^2y^0 + bxy^2 + b'xy + b''xy^0 + cx^0y^2 + c'x^0y + c''x^0y^0$$

Passo 3: Polinômio parcial resultante:

$$p_{\otimes}(x, y) = 2x^2y^2 + x^2 + y^2$$

Passo 4: Análise da variável ou termo oculto, cuja função é expressar o não-determinismo da Nmatriz.

- **As variáveis ocultas em um sistema trivalorado**

  Neste momento representaremos a característica principal das Nmatrizes por meio das variáveis ocultas. Analisando os polinômios de graus menores que três, já que o sistema é trivalorado, percebemos que:
  (I) O polinômio x^2 é restrito ao conjunto $\{0, 1\}$, pois para qualquer $x \in \{0, 1, 2\}$ temos que $x^2 \in \{0, 1\}$, ou seja:

  - Se $x = 0$, então $0^2 = 0$.
  - Se $x = 1$, então $1^2 = 1$.
  - Se $x = 2$, então $2^2 = 4 \equiv_{mod\ 3} 1$.

Pode haver outros polinômios restritos, obviamente, contudo para nossos propósitos basta lançar mão de um deles.

(II) O polinômio x^2+1 é restrito ao conjunto $\{1,2\}$, pois para qualquer $x \in \{0,1,2\}$ temos que $x^2+1 \in \{1,2\}$, ou seja:

- Se $x=0$, então $0^2+1=1$.
- Se $x=1$, então $1^2+1=2$.
- Se $x=2$, então $2^2+1=5 \equiv_{mod\ 3} 2$.

O mesmo ocorre para $2.(x^2+1)$, ou seja, para qualquer $x \in \{0,1,2\}$ temos que $2.(x^2+1) \in \{1,2\}$.

(III) O polinômio $2x^2$ é restrito ao conjunto $\{0,2\}$, pois para qualquer $x \in \{0,1,2\}$ temos que $2x^2 \in \{0,2\}$, ou seja:

- Se $x=0$, então $2.0^2=0$.
- Se $x=1$, então $2.1^2=2$.
- Se $x=2$, então $2.2^2=8 \equiv_{mod\ 3} 2$.

Diante desse contexto, representaremos o conjunto de valores de verdade $\{1,2\}$ das Nmatrizes, pelo seguinte polinômio com variáveis ocultas: (x'^2+1). O leitor poderá notar que nossa escolha em representar o conjunto $\{1,2\}$ por 1 é arbitrária (embora conveniente). Se tivéssemos representado $\{1,2\}$ por 2, bastaria aqui usar o polinômio $2(x'^2+1)$.

Além disso, como uma outra forma de realizar o passo 1, poderíamos ter optado em aplicar o método com a tabela preenchida por um dos possíveis polinômios restritos àquele determinado conjunto de valores de verdade. Assim, teríamos a seguinte tabela (optando pelo polinômio x'^2+1):

$\widetilde{\vee}$	0	2	1
0	$\{0\}$	x'^2+1	x'^2+1
2	x'^2+1	x'^2+1	x'^2+1
1	x'^2+1	x'^2+1	x'^2+1

Em (Carnielli 2007) (vide também teorema 1.4.1), Walter Carnielli mostrou, redescobrindo um provável resultado do folclore matemático, que toda função $A^m \to A$, para A finito, $|A|=k$,

pode ser expressa em termos de polinômios sobre o corpo $GF(p^n)$, para $k \leq p$. É facil mostrar que uma generalização desse teorema se aplica às matrizes não-determinísticas.

Teorema 3.3.1. *(Representação de funções finitas não-determinísticas em um corpo de Galois): Seja $\mathcal{M} = \langle \mathcal{V}, \mathcal{D}, \mathcal{O} \rangle$, uma matriz não-determinística (para uma linguagem $\mathcal{L}$). Então $\mathcal{M}$ pode ser descrita como polinômios sobre um corpo de Galois apropriado.*

Demonstração: Se cada função $\widetilde{\diamond} : \mathcal{V}^m \to 2^{\mathcal{V}} - \{\emptyset\}$ retorna apenas conjuntos unitários, trata-se de uma função determinística e o raciocínio é o mesmo do teorema 1.4.1.

Caso contrário, a função $\widetilde{\diamond}$ retorna, para uma entrada em $\mathcal{V}^m$, todas as funções sobrejetoras sobre um conjunto não-vazio C em $2^{\mathcal{V}} - \{\emptyset\}$.

Mas a classe de tais funções tem cardinalidade finita $|C|^{|\mathcal{V}|}$ e, portanto, pode ser expressa como polinômios sobre um corpo $GF(p^n)$ adequado (como segue imediatamente do teorema 1.4.1).

Basta, então, considerar a classe de todas as funções sobrejetoras com entrada $\mathcal{V}^m$ e saída V x $GF(p^n)[X']$, as quais continuam a ser expressas em termos polinomiais em razão do teorema 1.4.1. ∎

É importante notarmos que o número máximo de variáveis ocultas necessárias para a representação das entradas não-determinísticas em uma matriz finita e não-determinística, $\widetilde{\diamond} : \mathcal{V}^m \to 2^{\mathcal{V}} - \{\emptyset\}$ é, no pior caso (onde todas as entradas são não-determinísticas) limitado por $\mathcal{V}^m$. Isto é, o número máximo de variáveis ocultas que devem ser introduzidas no sistema resume-se ao número de valores de verdade de $\mathcal{V}$ elevado a n, onde n é a aridade da matriz.

3.3.2 Polinômios associados às tabelas de verdades dos operadores para $\mathcal{M}_{mbC}$.

Faremos, a partir de agora, uma mudança na notação dos valores de verdade das tabelas a fim de tornar o processo de cálculo dos sistemas menos complexo. Assim, uma Nmatriz para o sistema mbC é formado pela tripla $\mathcal{M} = \langle \mathcal{V}, \mathcal{D}, \mathcal{O} \rangle$, com a notação: $(f, t, I) = (0, 1, 2)$, em que:

- $\mathcal{V} = \{f, t, I\} = \{0, 1, 2\}$;
- $\mathcal{D} = \{t, I\} = \{1, 2\}$;
- $\mathcal{O}$ são operações definidas, matricialmente, por:

$\widetilde{\vee}$	0	2	1
0	$\{0\}$	$\{1,2\}$	$\{1,2\}$
2	$\{1,2\}$	$\{1,2\}$	$\{1,2\}$
1	$\{1,2\}$	$\{1,2\}$	$\{1,2\}$

$\widetilde{\wedge}$	0	2	1
0	$\{0\}$	$\{0\}$	$\{0\}$
2	$\{0\}$	$\{1,2\}$	$\{1,2\}$
1	$\{0\}$	$\{1,2\}$	$\{1,2\}$

$\widetilde{\rightarrow}$	0	2	1
0	$\{1,2\}$	$\{1,2\}$	$\{1,2\}$
2	$\{0\}$	$\{1,2\}$	$\{1,2\}$
1	$\{0\}$	$\{1,2\}$	$\{1,2\}$

$\widetilde{\neg}$	0	2	1
	$\{1,2\}$	$\{1,2\}$	$\{0\}$

$\widetilde{\circ}$	0	2	1
	$\{0,1,2\}$	$\{0\}$	$\{0,1,2\}$

O procedimento de obtenção dos referidos polinômios pode ser escrito com uma tabela bivalorada cujos valores de verdade sejam 1 e 0, com a finalidade de tornar o método, nestes casos, mais eficiente, como veremos. Diante disso, nos lugares onde houverem mais de um valor de verdade substituiremos estes valores por 1. Ao término do processo, com o polinômio pré-determinado, faremos as observações e mudanças necessárias para termos, de fato, um polinômio que traduza a tabela.

Logo, reescrevendo as tabelas acima temos:

$\widetilde{\vee}$	0	2	1
0	{0}	{1}	{1}
2	{1}	{1}	{1}
1	{1}	{1}	{1}

$\widetilde{\wedge}$	0	2	1
0	{0}	{0}	{0}
2	{0}	{1}	{1}
1	{0}	{1}	{1}

$\widetilde{\rightarrow}$	0	2	1
0	{1}	{1}	{1}
2	{0}	{1}	{1}
1	{0}	{1}	{1}

$\widetilde{\neg}$	0	2	1
	{1}	{1}	{0}

$\widetilde{\circ}$	0	2	1
	{1}	{0}	{1}

Assim, tornamos as tabelas bivaloradas e, portanto, a obtenção do polinômio ocorre conforme já explicado nas seções precedentes. Para este exemplo, faremos o procedimento em detalhes. Para os demais, apenas explicitaremos o polinômio final.

Como a o sistema é trivalorado os polinômios gerais que utilizaremos serão:
(i) $p(x) = ax^2 + bx + c$.
(ii)$p(x, y) = ax^2y^2 + a'x^2y + a''x^2y^0 + bxy^2 + b'xy + b''xy^0 + cx^0y^2 + c'x^0y + c''x^0y^0$.

1. **Polinômio para a disjunção.**

   A Nmatriz em mbC para o operador da disjunção é dada por:

$\widetilde{\vee}$	0	2	1
0	{0}	{1, 2}	{1, 2}
2	{1, 2}	{1, 2}	{1, 2}
1	{1, 2}	{1, 2}	{1, 2}

$\widetilde{\vee}$	0	2	1
0	{0}	{1}	{1}
2	{1}	{1}	{1}
1	{1}	{1}	{1}

   Analisando a tabela simplificada verificamos que:
   $p(0, 0) = 0$;
   $p(0, 2) = p(0, 1) = p(2, 0) = p(2, 2) = p(2, 1) = p(1, 0) = p(1, 2) = p(1, 1) = 1$.

   Logo, iniciando a substituição de cada um dos pontos no polinômio geral $p(x, y) = ax^2y^2 + a'x^2y + a''x^2y^0 + bxy^2 + b'xy + b''xy^0 + cx^0y^2 + c'x^0y + c''x^0y^0$, temos:
   (i) $p(0, 0) = 0 \Rightarrow a0^20^2 + a'0^20 + a''0^2 + b00^2 + b'00 + b''0 + c0^2 + c'0 + c'' = 0 \Rightarrow c'' = 0$.

   Reescrevendo o polinômio geral com o valor de c", temos:
   $p(x, y) = ax^2y^2 + a'x^2y + a''x^2 + bxy^2 + b'xy + b''x + cy^2 + c'y$.

(ii)$p(0,2) = 1 \Rightarrow cy^2 + c'y = 1 \Rightarrow c2^2 + c'2 = 1 \Rightarrow c + 2c' = 1.$
(iii)$p(0,1) = 1 \Rightarrow c1^2 + c'1 = 1 \Rightarrow c + c' = 1.$

$$\begin{cases} c + 2c' = 1 \\ c + c' = 1 \end{cases} \tag{3.14}$$

$$\begin{cases} c + 2c' = 1 \\ -c - c' = -1 \end{cases} \tag{3.15}$$

Pelo método da adição, $c' = 0$ e $c = 1$.

Assim, o polinômio geral com esses novos valores terá a seguinte configuração:
$p(x,y) = ax^2y^2 + a'x^2y + a''x^2 + bxy^2 + b'xy + b''x + y^2.$

(iv) $p(2,0) = 1 \Rightarrow a''x^2 + b''x = 1 \Rightarrow a''2^2 + b''2 = 1 \Rightarrow a'' + 2b'' = 1.$
Lembremos que, $2^2 = 4 \equiv_{mod3} 1.$
(v) $p(1,0) = 1 \Rightarrow a''1^2 + b''1 = 1 \Rightarrow a'' + b'' = 1.$

$$\begin{cases} a'' + 2b'' = 1 \\ a'' + b'' = 1 \end{cases} \tag{3.16}$$

Resolvendo o sistema, $b'' = 0$ e $a'' = 1$.

Assim, o polinômio geral terá a seguinte configuração:
$p(x,y) = ax^2y^2 + a'x^2y + x^2 + bxy^2 + b'xy + y^2.$

(vi) $p(2,2) = 1 \Rightarrow a2^22^2 + a'2^22 + 2^2 + b22^2 + b'22 + 2^2 = 1.$

$$a + 2a' + 2b + b' + 2 = 1$$

(vii) $p(2,1) = 1 \Rightarrow a2^21^2 + a'2^21 + 2^2 + b21^2 + b'21 + 1^2 = 1.$

$$a + a' + 2b + 2b' + 2 = 1$$

(viii) $p(1,2) = 1 \Rightarrow a1^22^2 + a'1^22 + 1^2 + b12^2 + b'12 + 2^2 = 1.$

$$a + 2a' + b + 2b' + 2 = 1$$

(ix) $p(1,1) = 1 \Rightarrow a1^21^2 + a'1^21 + 1^2 + b11^2 + b'11 + 1^2 = 1.$

$$a + a' + b + b' + 2 = 1$$

$$\begin{cases} a + 2a' + 2b + b' + 2 = 1 \\ a + a' + 2b + 2b' + 2 = 1 \\ a + 2a' + b + 2b' + 2 = 1 \\ a + a' + b + b' + 2 = 1 \end{cases} \tag{3.17}$$

Resolvendo este sistema temos o seguinte polinômio:

$$p(x, y) = 2x^2y^2 + x^2 + y^2$$

Lembremos que, ao iniciarmos o processo substituímos os valores $\{1, 2\}$ por $\{1\}$ na Nmatriz do operador da disjunção. Sendo assim, representaremos o conjunto de valores de verdade $\{1, 2\}$ das Nmatrizes, pelo seguinte polinômio com variáveis ocultas: $(x'^2 + 1)$. O leitor poderá notar que nossa escolha em representar o conjunto $\{1, 2\}$ por 1 é arbitrária (embora conveniente). Se tivéssemos representado $\{1, 2\}$ por 2, bastaria aqui usar o polinômio $2(x'^2 + 1)$.

Logo, o polinômio final para a Nmatriz de mbC em relação ao conectivo da disjunção é dado por:

$$p_\vee(x, y) = (2x^2y^2 + x^2 + y^2)\,(x'^2 + 1)$$

2. **Polinômio para a conjunção em mbC.**
A tabela para a Nmatriz do operador da conjunção é dada por:

$\widetilde{\wedge}$	0	2	1
0	$\{0\}$	$\{0\}$	$\{0\}$
2	$\{0\}$	$\{1, 2\}$	$\{1, 2\}$
1	$\{0\}$	$\{1, 2\}$	$\{1, 2\}$

Procedendo de modo análogo ao caso anterior temos o seguinte polinômio para a conjunção:

$$p_\wedge(x, y) = (x.y)\,(x'^2 + 1)$$

3. **Polinômio para o condicional em mbC.**
A tabela para a Nmatriz do operador condicional é dada por:

$\widetilde{\rightarrow}$	0	2	1
0	$\{1, 2\}$	$\{1, 2\}$	$\{1, 2\}$
2	$\{0\}$	$\{1, 2\}$	$\{1, 2\}$
1	$\{0\}$	$\{1, 2\}$	$\{1, 2\}$

O polinômio final para o operador condicional é dado por:

$$p_\rightarrow(x, y) = (x^2y^2 + 2x^2 + 1)\,(x'^2 + 1)$$

4. **Polinômio para a negação em mbC.**
   A tabela para a Nmatriz do operador da negação é dada por:

$\widetilde{\neg}$	0	2	1
	$\{1,2\}$	$\{1,2\}$	$\{0\}$

   O polinômio final para o operador da negação é dado por:

$$p_{\neg}(x) = (x^2 + x + 1)\,(x'^2 + 1)$$

5. **Polinômio para o operador da consistência em mbC.**
   A tabela para a Nmatriz do operador da consistência é dada por:

$\widetilde{\circ}$	0	2	1
	$\{0,1,2\}$	$\{0\}$	$\{0,1,2\}$

   O polinômio final para o operador da consistência é dado por:

$$p_{\circ}(x) = (x^2 + 2x + 1)\,(x')$$

Em resumo, temos:
$p_{\vee}(x,y) = (2x^2y^2 + x^2 + y^2)\,(x'^2 + 1)$;
$p_{\wedge}(x,y) = (x.y)\,(x'^2 + 1)$;
$p_{\rightarrow}(x,y) = (x^2y^2 + 2x^2 + 1)\,(x'^2 + 1)$;
$p_{\neg}(x) = (x^2 + x + 1)\,(x'^2 + 1)$;
$p_{\circ}(x) = (x^2 + 2x + 1)\,(x')$.

Assim como foi feito nos teoremas 1.3.9, 2.3.14 e 3.3.1, o que concluímos é que os polinômios acima oferecem uma representação polinomial para a estrutura que Arnon Avron denomina "non-deterministic matrix"(Nmatrizes) em (Avron 2007), seção 3. A partir daí fica claro que nosso enfoque produz uma representação correta e completa para a semântica do sistema mbC.

3.3.3 Uma versão polinomial da lógica paraconsistente mCi em Nmatrizes

Uma Nmatriz para a lógica mCi, em uma linguagem $\mathcal{L} = \{\wedge, \vee, \rightarrow, \neg, \circ\}$ é composta por $\mathcal{M}_{mCi} = \langle \mathcal{V}, \mathcal{D}, \mathcal{O} \rangle$, em que $(T, t, I, F, f) = (4, 3, 2, 1, 0)$, e:

- $\mathcal{V} = \{T, t, I, F, f\} = \{4, 3, 2, 1, 0\}$.
- $\mathcal{D} = \{I, T, t\} = \{2, 3, 4\}$
- Os operadores em $\mathcal{O}$ são definidos, matricialmente, por:
  (i) Disjunção.

$\widetilde{\vee}$	0	1	2	3	4
0	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
1	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
2	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
3	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
4	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$

(ii) Conjunção.

$\widetilde{\wedge}$	0	1	2	3	4
0	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
1	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
2	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
3	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
4	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$

(iii) Condicional.

$\widetilde{\rightarrow}$	0	1	2	3	4
0	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
1	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
2	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
3	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
4	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$

(iv) Negação.

$\widetilde{\neg}$	0	1	2	3	4
	$\{2,3\}$	$\{4\}$	$\{2,3\}$	$\{0\}$	$\{1\}$

(v) Consistência.

$\widetilde{\circ}$	0	1	2	3	4
	$\{4\}$	$\{4\}$	$\{1\}$	$\{4\}$	$\{4\}$

A obtenção do polinômio será análoga a realizada para o sistema mbC, ou seja:

1. Inicialmente, tornamos as matrizes bivaloradas, ou seja, no espaço onde houver $\{2,3\}$ substituiremos pelo valor 1 (ou pelo polinômio com variável oculta $x'^4 + 2$), exceto para os operadores de negação e consistência.

2. Para cada operador, a partir do polinômio geral para um sistema pentavolorado, aplicamos ponto a ponto as combinações bivalentes dos valores de verdade (quando os operadores forem bivalentes) ou então os valores unários para operadores unários, determinando assim um sistema linear.

3. Ao término da resolução do sistema, encontraremos o polinômio parcial do operador em análise.

4. Por fim, analisa-se os valores das Nmatrizes em função das variáveis ocultas.

Assim, temos:

- **Polinômio para a Disjunção em mCi.**
  (1) Reescrevendo a tabela, temos:

$\widetilde{\vee}$	0	1	2	3	4
0	{0}	{0}	{1}	{1}	{1}
1	{0}	{0}	{1}	{1}	{1}
2	{1}	{1}	{1}	{1}	{1}
3	{1}	{1}	{1}	{1}	{1}
4	{1}	{1}	{1}	{1}	{1}

(2,3) Aplicando o polinômio geral e encontrando as equações do sistema linear:

Polinômio geral: $p(x,y) = ax^4y^4 + a'x^4y^3 + a''x^4y^2 + a'''x^4y + a''''x^4y^0 + bx^3y^4 + b'x^3y^3 + b''x^3y^2 + b'''x^3y + b''''x^3y^0 + cx^2y^4 + c'x^2y^3 + c''x^2y^2 + c'''x^2y + c''''x^2y^0 + dxy^4 + d'xy^3 + d''xy^2 + d'''xy + d''''xy^0 + ex^0y^4 + e'x^0y^3 + e''x^0y^2 + e'''x^0y + e''''x^0y^0$.

Temos que:
$p(0,0) = p(0,1) = p(1,0) = p(1,1) = 0$.

$p(0,2) = p(0,3) = p(0,2) = p(0,4) = p(1,2) = p(1,2) = p(1,3) = p(1,4) = p(2,0) = p(2,1) = p(2,2) = p(2,3) = p(2,4) = p(3,0) = p(3,1) = p(3,2) = p(3,3) = p(3,4) = p(4,0) = p(4,1) = p(4,2) = p(4,3) = p(4,4) = 1$.

O polinômio parcial é dado por:

$p_\vee(x,y) = x^4y^4 + 3x^4y^3 + 3x^4y^2 + 3x^4y + 2x^4 + 3x^3y^4 + 4x^3y^3 + 4x^3y^2 + 4x^3y + x^3 + 3x^2y^4 + 4x^2y^3 + 4x^2y^2 + 4x^2y + x^2 + 3xy^4 + 4xy^3 + 4xy^2 + 4xy + x + 2y^4 + y^3 + y^2 + y$.

Simplificando temos:
$p_\vee(x,y) = \left((x.\,(x+4))^4 + (y.\,(y+4))^4\right)^4$.

(iv) O polinômio $(x'^4 + 2)$ representa o conjunto de valores de verdade $\{2,3\}$. Assim, o polinômio final, no modelo simplificado, é dado por:

$p_\vee(x,y) = \left(\left((x.\,(x+4))^4 + (y.\,(y+4))^4\right)^4\right)(x'^4 + 2)$.

- **Polinômio para a Conjunção em mCi.**

A tabela para a Nmatriz do operador da conjunção é dada por:

$\widetilde{\wedge}$	0	1	2	3	4
0	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
1	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
2	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
3	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
4	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$

Procedendo de modo análogo ao caso anterior temos o seguinte polinômio para a conjunção:

$$p_{\wedge}(x,y) = 4x^4y^4 + 2x^4y^3 + 2x^4y^2 + 2x^4y + 2x^3y^4 + x^3y^3 + x^3y^2 + x^3y + 2x^2y^4 + x^2y^3 + x^2y^2 + x^2y + 2xy^4 + xy^3 + xy^2 + xy$$

Simplificando e reescrevendo tendo em conta as variáveis ocultas temos:
$p_{\wedge}(x,y) = ((x+4)(y+4))^4 (x'^4 + 2)$.

- **Polinômio para o Condicional em mCi.**
A tabela para a Nmatriz do operador condicional é dada por:

$\widetilde{\rightarrow}$	0	1	2	3	4
0	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
1	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
2	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
3	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$
4	$\{0\}$	$\{0\}$	$\{2,3\}$	$\{2,3\}$	$\{2,3\}$

Procedendo de modo análogo ao caso anterior temos o seguinte polinômio:

$$p_{\rightarrow}(x,y) = (4x^4y^4 + 2x^4y^3 + 2x^4y^2 + 2x^4y + 3x^4 + 2x^3y^4 + 1x^3y^3 + 1x^3y^2 + 1x^3y + 4x^3 + 2x^2y^4 + 1x^2y^3 + 1x^2y^2 + 1x^2y + 4x^2 + 2xy^4 + 1xy^3 + 1xy^2 + 1xy + 4x + 1)(x'^4 + 2)$$

- **Polinômio para a negação em mCi.**
A tabela para a Nmatriz do operador da negação é dada por:

$\widetilde{\neg}$	0	1	2	3	4
	$\{2,3\}$	$\{4\}$	$\{2,3\}$	$\{0\}$	$\{1\}$

O polinômio final para o operador da negação é dado por:

$$p_{\neg}(x) = (x(x+3)^2(x+2)^2 + (x+1)^2(x+2)^2(x+4)^2(x'^4+2))$$

- **Polinômio para o operador da consistência em mCi.**
  A tabela para a Nmatriz do operador da consistência é dada por:

$\widetilde{\circ}$	0	1	2	3	4
	$\{4\}$	$\{4\}$	$\{1\}$	$\{4\}$	$\{4\}$

  O polinômio final para o operador da consistência é dado por:

$$p_{\circ}(x) = (3x^4 + x^3 + 2x^2 + 4x + 4)$$

Novamente, assim como foi feito nos teoremas 1.3.9 e 2.4.5, o que concluímos é que os polinômios acima oferecem uma representação polinomial para a estrutura que Arnon Avron denomina "non-deterministic matrix"(Nmatrizes) em (Avron 2008). A partir daí fica claro que nosso enfoque produz uma representação correta e completa para a semântica do sistema mCi.

3.3.4 Uma versão polinomial para a maioria das LFIs

Seja $\mathcal{S} = \{i, c, e, ci, ie, ce, cie, ia, cia, iae, ciae, io, cio, ioe, cioe\}$.

- Para $s \in \mathcal{S}$, uma mbCs-Nmatriz é uma mbC-Nmatriz que satisfaz a *Cond(x)* para todo x que ocorre em s.

  As condições em mbC-Nmatrizes que correspondem aos axiomas (i), (c), (e), (a) e (o) são as seguintes:
  Cond(i): $a \in \mathcal{T} \cup \mathcal{F} \Rightarrow \widetilde{\circ}a \subseteq \mathcal{T}$
  Cond(c): $a \in \mathcal{F} \Rightarrow \widetilde{\neg}a \subseteq \mathcal{T}$
  Cond(e): $a \in \mathcal{I} \Rightarrow \widetilde{\neg}a \subseteq \mathcal{I}$
  Cond(a): $a \in \mathcal{T} \cup \mathcal{F}$, e $b \in \mathcal{T} \cup \mathcal{F} \Rightarrow a\widetilde{\sharp}b \subseteq \mathcal{T} \cup \mathcal{F}, (\sharp \in \{\vee, \wedge, \rightarrow\})$
  Cond(o): $a \in \mathcal{T} \cup \mathcal{F}$ ou $b \in \mathcal{T} \cup \mathcal{F} \Rightarrow a\widetilde{\sharp}b \subseteq \mathcal{T} \cup \mathcal{F}, (\sharp \in \{\vee, \wedge, \rightarrow\})$

- $\mathcal{M}_{mbCs}$ é a única mbCs-Nmatriz em que $\mathcal{T} = \{t\}$, $\mathcal{F} = \{f\}$ e $\mathcal{I} = \{I\}$, onde $(f, I, t) = (0, 2, 1)$.

Os anéis de polinômios definidos para as mbCs-Nmatrizes são dados por:

1. Se o axioma (i) ocorre em s, então a tabela de verdade de $\mathcal{M}_{mbCs}$ correspondente ao conectivo $\circ$ é dada por:

$\widetilde{\circ}$	f	I	t
	$\{t\}$	$\{f\}$	$\{t\}$

   O polinômio associado a este operador é dado por:

$$\widetilde{o}(x) = x^2 + 2x + 1$$

2. Em $\mathcal{M}_{mbCc}$, $\mathcal{M}_{mbCci}$, $\mathcal{M}_{mbCcia}$ e $\mathcal{M}_{mbCcio}$ a tabela de verdade correspondente ao conectivo $\neg$ é dada por:

$\widetilde{\neg}$	f	I	t
	$\{t\}$	$\{I,t\}$	$\{f\}$

O polinômio associado a este operador é dado por:

$$\widetilde{\neg}(x) = (2x+1) + x(x+2)(x'^2)$$

3. Em $\mathcal{M}_{mbCe}$, $\mathcal{M}_{mbCie}$, $\mathcal{M}_{mbCiae}$ e $\mathcal{M}_{mbCioe}$ a tabela de verdade corresponde ao conectivo $\neg$ é dada por:

$\widetilde{\neg}$	f	I	t
	$\{I,t\}$	$\{I\}$	$\{f\}$

O polinômio associado a este operador é dado por:

$$\widetilde{\neg}(x) = (2x+1) + (x+2)(x+1)(x'^2 + x')$$

4. Em $\mathcal{M}_{mbCce}$, $\mathcal{M}_{mbCcie}$, $\mathcal{M}_{mbCciae}$ e $\mathcal{M}_{mbCcioe}$ a tabela de verdade correspondente ao conectivo $\neg$ é dada por:

$\widetilde{\neg}$	f	I	t
	$\{t\}$	$\{I\}$	$\{f\}$

O polinômio associado a este operador é dado por:

$$\widetilde{\neg}(x) = 2x+1$$

5. Se **a** ocorre em s, então a tabela de verdade de $\mathcal{M}_{mbCs}$ correspondente aos conectivos $\{\vee, \wedge, \rightarrow\}$ é dada por:

$\widetilde{\vee}$	f	I	t
f	$\{f\}$	$\{I,t\}$	$\{t\}$
I	$\{I,t\}$	$\{I,t\}$	$\{I,t\}$
t	$\{t\}$	$\{I,t\}$	$\{t\}$

$\widetilde{\wedge}$	f	I	t
f	$\{f\}$	$\{f\}$	$\{f\}$
I	$\{f\}$	$\{I,t\}$	$\{I,t\}$
t	$\{f\}$	$\{I,t\}$	$\{t\}$

$\widetilde{\rightarrow}$	f	I	t
f	$\{t\}$	$\{I,t\}$	$\{t\}$
I	$\{f\}$	$\{I,t\}$	$\{I,t\}$
t	$\{f\}$	$\{I,t\}$	$\{t\}$

Os polinômios associados a esses operadores são:

$$p_{\widetilde{\vee}}(x,y) = (2xy+x+y)(2x^2y+2xy^2+xy+2x^2+2x+2y^2+2y) + (2x^2y^2+x^2y+xy^2+2xy+2x^2+2y^2+x+y)(x'^2+1)$$
$$p_{\widetilde{\wedge}}(x,y) = (x^2y^2+x^2y+xy^2+xy) + (2x^2y+2xy^2+2xy)(x'^2+1)$$
$$p_{\widetilde{\rightarrow}}(x,y) = (2x^2y+2x^2+xy^2+xy+y^2+2y+1) + (x^2y^2+x^2y+2xy^2+2xy+2y^2+y)(x'^2+1)$$

6. Se **o** ocorre em s, então a tabela de verdade de $\mathcal{M}_{mbCs}$ correspondente aos conectivos $\{\vee, \wedge, \rightarrow\}$ é dada por:

$\widetilde{\vee}$	f	I	t
f	$\{f\}$	$\{t\}$	$\{t\}$
I	$\{t\}$	$\{I,t\}$	$\{t\}$
t	$\{t\}$	$\{t\}$	$\{t\}$

$\widetilde{\wedge}$	f	I	t
f	$\{f\}$	$\{f\}$	$\{f\}$
I	$\{f\}$	$\{I,t\}$	$\{t\}$
t	$\{f\}$	$\{t\}$	$\{t\}$

$\widetilde{\rightarrow}$	f	I	t
f	$\{t\}$	$\{t\}$	$\{t\}$
I	$\{f\}$	$\{I,t\}$	$\{t\}$
t	$\{f\}$	$\{t\}$	$\{t\}$

Os polinômios associados a esses conectivos são dados por:

$$p_{\widetilde{\vee}}(x,y) = (x^2y^2 + x^2y + x^2 + xy^2 + 2xy + y^2) + (x^2y^2 + 2x^2y + 2xy^2 + xy)(x'^2 + 1)$$
$$p_{\widetilde{\wedge}}(x,y) = (x^2y + xy^2 + 2xy) + (x^2y^2 + 2x^2y + 2xy^2 + xy)(x'^2 + 1)$$
$$p_{\widetilde{\rightarrow}}(x,y) = (x^2y + 2x^2 + xy^2 + 2xy + 1) + (x^2y^2 + 2x^2y + 2xy^2 + xy)(x'^2 + 1)$$

Novamente, assim como foi feito nos teoremas 1.3.9, 2.5.6, 2.5.8 e 2.5.10 o que concluímos é que os polinômios acima oferecem uma representação polinomial para a estrutura que Arnon Avron denomina "non-deterministic matrix"(Nmatrizes) em (Avron 2007). A partir daí fica claro que nosso enfoque produz uma representação correta e completa para a semântica da maioria das LFIs.

Os principais resultados apresentados neste capítulo serão publicados em um artigo, em janeiro de 2014, no Anais do LSFA - 8 th Workshop on Logical and Semantic Frameworks, with Applications - sob o título: *Non-deterministic Semantics in Polynomial Format*.

3.4 O software PoLCa

O software PoLCa[4] é um programa que traduz sentenças dos mais diferentes sistemas lógicos (tais como multivalorados, paraconsistentes, etc.), cujas semânticas são determinísticas ou não-determinísticas, em anéis de polinômios com coeficientes em corpos finitos (corpos de Galois), automatizando assim todos os casos vistos nos exemplos acima. Provas em tais sistema reduzem-se, então, a manipulação intuitiva e natural de polinômios.

Resumidamente, dado uma coleção de tabelas de verdade, descritas por matrizes determinísticas ou não-determinísticas (Nmatrizes) que definem operadores lógicos de aridades arbitrárias, o software PoLCa (Polynomial Ring Calculus Software) computa os polinômios cujas variáveis inteiras representam os argumentos dos operadores lógicos, de modo que tais polinômios simulam todos os valores de entrada/saída da correspondente (determinística ou não-determinística) tabela de verdade. A corretude do programa é garantida pelos teoremas 1.4.1 e 3.3.1.

A entrada do programa é escrita em arquivo de texto, onde são especificadas as N-matrizes dos operadores de interesse. O interessante é que múltiplos operadores lógicos podem ser dados

[4]Programado por Glauber De Bona e desenvolvido por Mariana Matulovic e Walter Carnielli.

no mesmo arquivo de entrada, desde que o número de valores de verdade seja o mesmo para todos.

A primeira linha (cabeçalho) do arquivo deve especificar, nesta ordem, o número de valores de verdade, o número de operadores lógicos cujas N-matrizes serão especificadas e a aridade de cada um dos operadores. Tais valores devem ser especificados com números naturais separados por espaço(s). Por exemplo, se o sistema possui dois operadores, um ternário e um unário, em uma lógica com cinco valores de verdade, a primeira linha do arquivo de entrada deve conter:

5 2 3 1 (cinco valores de verdade, dois operadores, aridade dos operadores (neste caso, respectivamente, três e um)

Em uma lógica com n valores de verdade, estes valores serão representados por números naturais 0,1,2...,n-1. Se o operador é unário, basta especificar os valores da aplicação do operador a 0,1,...n-1, usando números entre espaços. Por exemplo, consideremos a seguinte tabela de verdade para o operador unário o(x):

x	0	1	2
$o(x)$	1	0	2

Ele será representado, no programa, pela linha:

1 0 2

Para um operador o() de aridade m, com n valores de verdade, especificam-se recursivamente as n tabelas do operador o'() de aridade m-1, quando o primeiro argumento de o() é fixado em 0,1,...,n-1. Novamente usam-se inteiros entre espaços. Quebras de linha podem sempre ser adicionadas arbitrariamente, facilitando a formatação. Por exemplo, dada a tabela verdade de um operador binário, com argumentos x e y,

x/y	0	1	2
0	0	1	1
1	0	1	2
2	1	2	2

a representaríamos por:

0 1 1
0 1 2
1 2 2

Para representar conjuntos de valores (valores não determinísticos) nas tabelas, basta colocar os elementos do conjunto entre chaves separados por vírgula. Por exemplo, se para determinados valores de seus argumentos um operador pode levar aos valores 1 ou 2, coloca-se na repectiva posição de sua N-matriz $\{1, 2\}$.

Um arquivo de entrada exemplo, para uma lógica com três valores de verdade, um operador unário e um binário, poderia ser:

3 2 1 2

$\{1, 2\}$ 0 $\{1, 2\}$

1 0 1
$\{1, 2\}$ 0 $\{0, 1\}$
$\{2, 0\}$ 1 $\{1, 0, 2\}$

A saída do programa também é puramente textual. Para cada operador cuja tabela verdade (ou N-matriz) foi especificada na entrada, um polinômio separado é retornado. As variáveis são letras que seguem ordem alfabética refletindo a ordem dos argumentos implícita na especificação das tabelas verdade da entrada, conforme explicado acima.

Os polinômios são especificados em parcelas, uma correspondendo aos valores determinísticos da tabela verdade diferentes de zero (se houver), e cada uma das demais correspondendo a cada entrada não determinística da tabela verdade (se houver). Cada parcela referente a uma entrada não determinística é dada em dois fatores, onde o segundo representa a entrada não determinística, usando uma variável oculta x_a. Assim, para parcelas correspondentes a entradas não determinísticas, o primeiro fator é um polinômio que leva a 0 ou 1, e o segundo fator leva ao conjunto de valores pela variável oculta (note que tal fator não é único, havendo possivelmente mais de um polinômio com variável oculta que representa o mesmo conjunto de valores).

Todos os anéis de polinômios apresentados neste capítulo foram calculados manualmente e, eventualmente, como no caso da lógica mCi (pentavalorada), com o auxílio do Mathematica. Após o desenvolvimento do PoLCa, os resultados foram conferidos e arrumados (quando necessário).

Para maiores detalhes, veja:
http : *//marianamatulovic.wix.com/polyringcalculus*

Capítulo 4

A tese de Suszko e os Anéis de Polinômios

> "How was it possible that the humbug of many logical values persisted over the last fifty years?" (Roman Suszko in 22^{nd} *Conference on the History of Logic*).

Enquanto que, no capítulo anterior desenvolvemos um anel de polinômios para sistemas cuja verofuncionalidade foi generalizada por meio das matrizes não-determinísticas, neste capítulo centramos nosso interesse nos sistemas cuja verofuncionalidade foi perdida quando reduzidos pela chamada Redução de Suszko.

Assim, nossa contribuição foi definir, minuciosamente, os anéis de polinômios para os sistemas reduzidos pela Redução de Suszko (especificamente, as lógicas paraconsistentes P_3^1, P_4^1, LFI1 e lógica de Belnap, e consequentemente os teoremas 4.3.1, 4.3.2, 4.3.4 e 4.3.5) , os quais foram apresentados no artigo *Two's company: "The humbug of many logical values"*, (Caleiro et al. 2005), de Carlos Caleiro, Walter Carnielli, Marcelo Coniglio e João Marcos.

4.1 A tese de Suszko

Em 1976, durante uma conferência em Cracóvia (Polônia), o lógico polonês Roman Suszko reclama que mesmo depois de 50 anos do desenvolvimento das lógicas multivaloradas de Jan Łukasiewicz, ainda persistimos em trabalhar com uma das maiores fraudes conceituais desenvolvida em lógica matemática até os dias de hoje: as multivalorações. Para Suszko só há dois valores de verdade na lógica: o verdadeiro e o falso, e qualquer multiplicação de valores lógicos seria uma péssima ideia. A tese filosófica subjacente a esta afirmação é decorrente da distinção existente entre os *valores de verdade algébricos* e os *valores de verdade lógicos*. Para Suszko, enquanto os *valores de verdade algébricos* possuem um objetivo meramente referencial, os *valores de verdade lógicos*, aqueles que de fato existem, resumem-se a apenas dois valores: o verdadeiro e o falso. Na realidade, trata-se de uma atualização e ampliação da discriminação Fregeana entre o sentido e a referência de conceitos saturados.

A Tese de Suszko, grosseiramente, nos diz que toda lógica tarskiana multivalorada pode ser caracterizada por uma lógica bivalorada. Na realidade Suszko ilustra sua proposição demonstrando como a lógica trivalorada de Łukasiewicz, $Ł_3$, pode ser tratada em função de uma semântica não-verofuncional e bivalorada.

A fim de que possamos realizar a tradução polinomial dos sistemas reduzidos *à la* Suszko com maior clareza, iniciamos este capítulo com a definição do procedimento de transformação de um sistema multivalorado em bivalorado. Além disso, discutiremos as principais diferenças entre as formas polinomiais das traduções desses sistemas antes e depois da redução de Suszko.

4.2 Procedimento de transformação de um sistema n-valorado em bivalorado.

Nesta seção, faremos uma reescrita do artigo *Two's company: "The humbug of many logical values"*, (Caleiro et al. 2005), a fim de que possamos deixar claro ao leitor como é realizada a mudança de valência aos moldes de Suszko. Diante disso, a maioria das definições e conceitos apresentados aqui são idênticos ao original. Ocorre que, a fim de tornar o texto mais compreensível aos leitores, tal conceitualização será essencial.

A ideia básica do método centra-se na separação os valores de verdade do sistema em distinguidos e não-distinguidos por meio da utilização de recursos linguísticos e, logo após esse processo, na tradução sintática das características das matrizes de n-valores de verdade, por meio de cláusulas, em um ambiente bivalorado.

4.2.1 Definições e conceitos importantes.

Denotemos $\mathcal{S}$ como um conjunto não-vazio de fórmulas e $\mathcal{V}$, também um conjunto não-vazio, de valores de verdade, tal que $\mathcal{V} = \mathcal{D} \cup \mathcal{U}$, onde $\mathcal{D} = \{d_1, d_2, ...\}$ é um conjunto de valores ditos *distinguidos* e $\mathcal{U} = \{u_1, u_2, ...\}$ um conjunto de valores *não-distinguidos*. É importante salientarmos que $\mathcal{D}$ e $\mathcal{U}$ são conjuntos disjuntos, ou seja, $\mathcal{D} \cap \mathcal{U} = \emptyset$.

Uma *n-valoração* é um mapeamento do conjunto de fórmulas $\mathcal{S}$ no conjunto de valores de verdade $\mathcal{V}$, ou seja:

$$\S_k^{\mathcal{V}} : \mathcal{S} \to \mathcal{V}_k, \text{ onde } n \text{ está em } |\mathcal{V}_k| \text{ e a cardinalidade de } \mathcal{V}_k \text{ é: } |\mathcal{V}_k| = |\mathcal{D}_k \cup \mathcal{U}_k|.$$

Se tanto $\mathcal{D}_k$ quanto $\mathcal{U}_k$ forem conjuntos unitários, ou seja, $\mathcal{D}_k = \{a\}$ e $\mathcal{U}_k = \{b\}$, com $a \neq b$, então $\S_k^{\mathcal{V}}$ será uma bivaloração. Um exemplo clássico é a bivaloração $\mathcal{V} = \{0, 1\}$, em que $\mathcal{D} = \{1\}$ e $\mathcal{U} = \{0\}$.

Uma *teoria* será qualquer conjunto Γ tal que $\Gamma \subseteq S$.

Definimos como uma *semântica n-valorada* qualquer coleção de valorações, denotada por *SEM*, onde n é a cardinalidade do maior $\mathcal{V}_k$ tal que $\S_k^{\mathcal{V}} \in SEM$.

Um *modelo* para uma fórmula φ é qualquer valoração $\S_k^{\mathcal{V}}$ tal que:

$$\S_k^{\mathcal{V}} : \mathcal{S} \to \mathcal{D}$$
$$\varphi \to \S_k^{\mathcal{V}}(\varphi) \in \mathcal{D}_k$$

Uma fórmula φ é consequência semântica de um conjunto de fórmulas $\Gamma \subseteq \mathcal{S}$ se, todos os modelos, de todas as fórmulas de Γ, são também modelos de φ, isto é:

$$\Gamma \models_{SEM} \varphi \text{ sse } \S_k^{\mathcal{V}}(\varphi) \in \mathcal{D}_k,$$

sempre que $\S_k^{\mathcal{V}}(\Gamma) \subseteq \mathcal{D}_k$ para toda valoração $\S_k^{\mathcal{V}} \in SEM$.

Em se tratando de uma relação abstrata de consequência, consideraremos as propriedades de inclusão, diluição e corte definidas no capítulo 2, seção 2.2, p. 39.

Para esta seção, definiremos uma lógica $\mathcal{L}$ como um conjunto de fórmulas munido com uma relação de consequência. Uma lógica será dita *tarskiana* se ela possuir como axiomas as propriedades de inclusão, diluição e corte. Em particular, quando SEM é um conjunto unitário também temos definido uma lógica tarskiana.

Para uma dada lógica $\mathcal{L} = \langle S, \Vdash \rangle$, uma teoria Γ, $\Gamma \subseteq S$, será denominada *fechada* se ela contém todas as suas consequências; o fecho de uma teoria Γ, denotado por $\bar{\Gamma}$, é dado por:

$$\varphi \in \bar{\Gamma} \text{ sse } \Gamma \Vdash \varphi$$

Uma *matriz de Lindenbaum* para uma teoria Γ é definida se considerarmos $\mathcal{V} = \mathcal{S}$, $\mathcal{D} = \bar{\Gamma}$ e $SEM[\Gamma] = \{id_s\}$ (a identidade mapeada no conjunto de fórmulas).

Como consequência disso, temos os famosos *Resultados de Redução*, que se caracterizam por:

Redução de Wójcicki
(RW): Toda lógica tarskiana $\mathcal{L} = \langle S, \Vdash \rangle$ é n-valorada, para algum $n \leq |S|$.

Redução de Suszko
(RW): Toda lógica tarskiana n-valorada pode ser caracterizada como bivalorada.

Analisando a *Redução de Wójcicki* percebemos que ela esboça a concepção de que há uma matriz característica, infinito valorada, em qualquer lógica tarskiana. Apesar dessa multiplicidade de valores de verdade permitidos pelas semânticas multivaloradas, devemos salientar que tais semânticas possuem uma notável sombra de bivalência em sua constituição, a qual nos permitirá distinguir os valores de verdade em distinguidos e não-distinguidos.

Nas palavras de Caleiro e Marcos, (Caleiro & Marcos 2010), p. 01:

> In spite of the multiplication of truth-values, a noticeable shade of bivalence lurks behind the canonical notion of entailment that many-valued logics inherit from 2-valued case.

Em relação à redução de Suszko, parece um tanto paradoxal que um mesmo sistema lógico seja caracterizado por duas semânticas bem distintas: uma n-valorada e uma bivalorada. Esta tensão é resolvida quando percebemos que tudo está atrelado a um conflito existente entre verofuncionalidade algébrica e bivalência. Exporemos mais sobre esse assunto quando tratarmos da verofuncionalidade, ou perda dela, nas transformações das valências semânticas.

4.2.2 Separação dos Valores de Verdade

Antes de apresentarmos a definição da separação dos valores de verdade, algumas definições e notações para a estrutura padrão do conjunto de fórmulas, de valores de verdade, entre outros, são necessárias neste momento. Assim, sejam $ats = \{p_1, p_2, ...\}$ um conjunto enumerável de *sentenças atômicas* e $\Sigma = \{\Sigma_n\}_{n\in\mathbb{N}}$ uma assinatura proposicional, em que cada Σ_n é um conjunto de *conectivos* de aridade n. Seja $cct = \bigcup_{n\in\mathbb{N}} \Sigma_n$, o conjunto de todos os conectivos. Diante disso,

o conjunto de fórmulas $\mathcal{S}$ é então definido como a álgebra livremente gerada pelas sentenças atômicas sobre Σ.

Seja $\mathcal{V}$ um conjunto não-vazio de valores de verdade, tal que $\mathcal{V} = \mathcal{D} \cup \mathcal{U}$, onde $\mathcal{D} = \{d_1, d_2, ...\}$ é um conjunto de valores ditos *distinguidos* e $\mathcal{U} = \{u_1, u_2, ...\}$ um conjunto de valores *não-distinguidos*. As valorações que compõem a semântica dos sistemas genuinamente n-valorados é dada pelo homomorfismo $\S : \mathcal{S} \to \mathcal{V}$.

Uma *substituição uniforme* é um ϵ-endomorfismo $\epsilon : \mathcal{S} \to \mathcal{S}$. Denotaremos por $\varphi(p_1, ..., p_n)$ uma fórmula φ cujo conjunto de sentenças atômicas aparecem entre $(p_1, ..., p_n)$. A partir de agora escreveremos $\varphi(p_1/\alpha_1, ..., p_n/\alpha_n)$ a substituição uniforme de $(p_1, ..., p_n)$ por $(\alpha_1, ..., \alpha_n)$, ao invés de $\epsilon(\varphi(p_1, ..., p_n))$.

Observação 4.2.1. Seja $\mathcal{L}$ uma lógica n-valorada, cuja semântica é determinada por $\langle \mathcal{V}, cct, \mathcal{D} \rangle$. Denotaremos por $\mathcal{L}^c$ qualquer lógica n-valorada que estende, conservativamente, $\mathcal{L}$.

Definição 4.2.2. Para cada $n \in \mathbb{N}^+$ e $\vec{v} = (v_1, ..., v_n) \in \mathcal{V}^n$, definimos a *função interpretação* $[\cdot] : \mathcal{V}^n \to \mathcal{V}$ sobre S do seguinte modo:
i) $[p_k](\vec{v}) = v_k$, se $1 \leq k \leq n$;
ii) $[\otimes(\varphi_1, ..., \varphi_m)](\vec{v}) = \otimes([\varphi_1](\vec{v}), ..., [\varphi_m](\vec{v}))$, em que $\otimes$ é um conectivo m-ário.

Definição 4.2.3. Sejam $v_1, v_2 \in \mathcal{V}$. Dizemos que v_1 e v_2 estão **separados**, e denotamos por $v_1 \sharp v_2$, se v_1 e v_2 pertencem a diferentes classes de valores de verdade, ou seja:

$$v_1 \sharp v_2 \Leftrightarrow \begin{cases} v_1 \in \mathcal{D}, v_2 \in \mathcal{U} \\ ou \\ v_1 \in \mathcal{U}, v_2 \in \mathcal{D} \end{cases} \tag{4.1}$$

Dada alguma lógica n-valorada $\mathcal{L}$, há sempre uma fórmula $\varphi(p)$ de $\mathcal{L}^c$ tal que φ separa os valores de verdade v_1 e v_2, isto é, $[\varphi](v_1) \sharp [\varphi](v_2)$.

De modo análogo, poderíamos dizer que uma fórmula $\varphi(p)$ separa v_1 e v_2 se o valor de verdade obtido na tabela de verdade de φ quando p assume os valores v_1 e v_2 são separáveis.

Exemplo 4.2.4. Consideremos a lógica trivalorada de Łukasiewicz.

$$Ł_3 = \left\langle \left\{0, \tfrac{1}{2}, 1\right\}, \{\neg, \rightarrow\}, \{1\} \right\rangle.$$

As matrizes de valores de verdade para $Ł_3$ são obtidas mediante as seguintes operações sobre os valores de verdade:
$\neg v_1 := 1 - v_1$.
$(v_1 \rightarrow v_2) := \text{Min}(1; 1 - v_1 + v_2)$.

Construindo a matriz de valoração para os operadores da negação e do condicional, temos:

	$\neg$
1	0
0	1
$\frac{1}{2}$	$\frac{1}{2}$

$\rightarrow$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	$\frac{1}{2}$	1	1
1	0	$\frac{1}{2}$	1

Uma das funções que separa os valores de verdade é a fórmula $\varphi := \neg p_0$, pois:
$[\varphi](0) := \neg(0) = 1$.
$[\varphi](\frac{1}{2}) := \neg(\frac{1}{2}) = \frac{1}{2}$.
Logo, $\neg(0) = 1 \neq \frac{1}{2} = \neg(\frac{1}{2})$. Sendo assim, $\varphi := \neg p_0$ separa os valores de verdade 1 e $\frac{1}{2}$, ou seja, $1 \sharp \frac{1}{2}$.

Exemplo 4.2.5. Considere um sistema lógico cuja semântica é dada por: $\langle \{0, \frac{1}{2}, 1\}, \{\otimes\}, \{1\} \rangle$, sendo $\mathcal{V} = \{0, \frac{1}{2}, 1\}$, $\mathcal{D} = \{1\}$ e $\otimes$ definido por:
$v_1 \otimes v_2 = v_1$, se $v_1 = v_2$.
$v_1 \otimes v_2 = 1$, se $v_1 \neq v_2$.
Analisando a função $\varphi := \otimes$, verificamos que nenhuma fórmula semanticamente caracteriza por $\otimes$ pode separar os valores de verdade já que:
$[\varphi](0, \frac{1}{2}) = 1 = [\varphi](\frac{1}{2}, 0)$. Assim, $[\varphi](0, \frac{1}{2}) = [\varphi](\frac{1}{2}, 0)$.

Hipótese 4.2.6. (Separabilidade)
A partir deste ponto assumiremos que para qualquer lógica finita que considerarmos, todo par $\langle v_1, v_2 \rangle \in \mathcal{D}^2 \cup \mathcal{U}^2$, com $v_1 \neq v_2$, é efetivamente separável.

Esta hipótese segue do fato de que é possível classificar os valores de verdade em termos de conjuntos distinguidos (representado, neste momento, pelo valor lógico **V**) e não-distinguidos (representados por **U**). Veremos que, juntamente com a Hipótese da Separabilidade, a sombra da bivalência incorporada na distinção entre os valores de verdade em distinguidos e não-distinguidos nos permitirá reformular a semântica original n-valorada, usando no máximo dois valores de verdade.

Observação 4.2.7. Seja $t : \mathcal{V} \to \{V, F\}$ uma função tal que:

$$t(v) = V \text{ se e somente se, } v \in \mathcal{D}, \text{ para alguma lógica } \mathcal{L}.$$

Temos que φ separa v_1 e v_2 se $t([\varphi](v_1)) \neq t([\varphi](v_2))(**)$. A partir desse momento, podemos nos referir a função separadora (e não somente à fórmula separada).

Lembremos que, $\mathcal{V} = \mathcal{D} \cup \mathcal{U}$ e que $\mathcal{D} = \{d_1, ..., d_i\}$ e $\mathcal{U} = \{u_1, ..., u_j\}$.

Suponhamos agora que, φ_{mn} separa d_m e d_n (para $1 \leq m < n \leq i$) e ψ_{mn} separa u_m e u_n (para $1 \leq m < n \leq j$). Dado uma variável x e $d \in \mathcal{D}$, consideremos a equação:
$t([\varphi_{mn}](x)) = q^d_{mn}$, onde $q^d_{mn} = t([\varphi_{mn}](d))$. Observe que, $q^d_{mn} \in \{V, F\}$ e $q^{d_m}_{mn} \neq q^{d_n}_{mn}$, por $(**)$.

Assim, se $\vec{\varphi}_d(x)$ é a sequência $\left(t([\varphi_{mn}](x)) = q^d_{mn}\right)_{1 \leq m < n \leq i}$, o valor de verdade distinguido **d** pode ser caracterizado através da sequência de equações $Q_d(x) : (t(x) = V, \vec{\varphi}_d(x))$, onde a vírgula representa a conjunção. Isto é:

$$x = d \text{ sse } t(x) = V \wedge \textstyle\bigwedge_{1 \leq m < n \leq i} t([\varphi_{mn}](x)) = q^d_{mn}.$$

Em consequência disso, conseguimos caracterizar o valor de verdade distinguido **d** em termos dos membros de $\mathcal{D}$ e de $\mathcal{U}$, ou equivalentemente, em termos de V ou F, como desejávamos.

Analogamente, se:
r^u_{mn} é $t([\psi_{mn}](u))$ para $(1 \leq m < n \leq j)$ e $u \in \mathcal{U}$, então a sequência de equações $R_u(x) : (t(x) = F, \vec{\psi}_u(x))$ caracteriza **u** em termos de V e F, onde $(\vec{\psi}_u(x) = t([\psi_{mn}](x))) = r^u_{mn}, (1 \leq m < n \leq j)$. Isto é:

$$x = u \text{ sse } t(x) = F \wedge \bigwedge_{1 \leq m < n \leq j} t([\psi_{mn}](x)) = r^u_{mn}.$$

Assim:

- Se $\mathcal{D} = \{d\}$, então escrevemos $((x = d) \Leftrightarrow t(x) = V)$.
- Se $\mathcal{U} = \{u\}$, então escrevemos $((x = u) \Leftrightarrow t(x) = F)$.

Observação 4.2.8. (Redução de Suszko)
Consideremos as funções, $\S^{\mathcal{V}}_k : \mathcal{S} \to \mathcal{V}$ e $t : \mathcal{V} \to \{V, F\}$. A função composição, $b = t \circ \S$, dá-nos exatamente a **redução de Suszko**, isto é:

$$\S^{\mathcal{V}}_k : \mathcal{S} \to \mathcal{V}$$
$$t : \mathcal{V} \to \{V, F\}$$
$$b =_{def} t \circ \S : \mathcal{S} \to \{V, F\}$$

Isso significa que, em uma lógica n-valorada, a semântica de multivalores atribui, a cada fórmula do sistema, um dos valoes de verdade contidos no conjunto $\mathcal{V}$. Já a função t, atribui a cada um dos valores de verdade de $\mathcal{V}$, o valor V ou F, de acordo com as definições apresentadas na observação anterior, tal como:

$t(v) = V$ se e somente se, $v \in \mathcal{D}$, para uma fixada lógica $\mathcal{L}$.

$t(v) = F$ se e somente se, $v \in \mathcal{U}$, para uma fixada lógica $\mathcal{L}$.

Sendo assim, dado um sistema lógico que respeita a Hipótese da Separabilidade, Caleiro, Carnielli, Coniglio e João Marcos apresentam em (Caleiro et al. 2005), o modo pelo qual esta semântica bivalorada pode ser mecanicamente escrita em termos de *semântica diádica*. Para um estudo mais aprofundado do tema, recomendo consultar o referido artigo. Para dar continuidade a nossa exposição, abriremos mão de algumas demonstrações e definições que poderão carregar o texto com informações não tão necessárias para os nossos objetivos.

Em resumo, o método para a transformação de um sistema n-valorado em bivalorado pode ser esquematizado por:

1. Dado um sistema n-valorado, construimos as matrizes de valorações dos conectivos da assinatura em questão.
2. A partir disso, verificamos se existe uma função que separa os valores de verdade. Isso é importante para que possamos classificar os valores de verdade em distinguidos e não-distinguidos. Para tanto, precisamos analisar se existe, no mínimo, dois valores de verdade no sistema, que ao serem aplicados mediante uma função, retornam valores distintos.
3. A partir dessa classificação, analisamos a matriz de valorações mediante a seguinte função: $b : \mathcal{S} \to \{V, F\}$. Assim, se a valoração da variável proposicional na tabela for um valor distinguido, isto é, $\S(p) = 1$ e $\mathcal{D} = \{1\}$, então $b(p) = V$. Se $\S(p)$ fosse não distinguido, então $b(p) = F$.

4. Por fim, depois de realizadas todas as análises a respeito da função dos valores de verdade e da redução de Suszko realizada via função b, escrevemos as cláusulas da bivaloração por meio da utilização da Lógica de Primeira Ordem, manipulando e simplificando ao máximo as referidas cláusulas.

Vejamos como isso ocorre, de fato, nos exemplos abaixo.

Exemplo 4.2.9. A Lógica Paraconsistente P_3^1.

A lógica paraconsistente P_3^1 foi desenvolvida por Sette em (Sette 1973), a qual ele denominou P^1, representada por $P_3^1 = \left\langle \left\{0, \frac{1}{2}, 1\right\}, \{\neg, \rightarrow\}, \left\{\frac{1}{2}, 1\right\}\right\rangle$ e com as seguintes matrizes de valores de verdades para os conectivos em questão:

	$\neg$
0	1
$\frac{1}{2}$	1
1	0

$\rightarrow$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	0	1	1
1	0	1	1

O que pretendemos nesse momento é transformar essa lógica trivalente em uma bivalente, usando para isso o algoritmo de transformação, já definido, nos seguintes passos:
i) Dado uma lógica n-valorada $\mathcal{L}$, há sempre alguma fórmula $\varphi(p)$ de $\mathcal{L}$ que separa os valores de verdade v_1 e v_2 de modo que $[\varphi](v_1)\sharp[\varphi](v_2)$.
ii) Aplicaremos o mapeamento t: $\mathcal{V} \rightarrow \{V, F\}$, tal que $t(v) = V$ sse $v \in \mathcal{D}$
iii) Uma semântica de Gentzen para uma lógica $\mathcal{L}$ é um adequado conjunto de bivalorações $b : \mathcal{S} \rightarrow \{V, F\}$.

Diante disso, iniciemos o processo através da análise da separação dos valores de verdade. Temos que, a negação separa os valores de verdade $\frac{1}{2}$ e 1 pois:

$$v(\tfrac{1}{2}) = 1 \neq 0 = v(1).$$

Como o conjunto de distinguidos é formado por $\mathcal{D} = \left\{\frac{1}{2}, 1\right\}$, temos:

	$\neg$
0	1
$\frac{1}{2}$	1
1	0

- $x = 0 \Rightarrow x \notin \mathcal{D} \Rightarrow t(x) = F, t(\neg x) = V$
- $x = \frac{1}{2} \Rightarrow x \in \mathcal{D} \Rightarrow t(x) = V, t(\neg x) = V$
- $x = 1 \Rightarrow x \in \mathcal{D} \Rightarrow t(x) = V, t(\neg x) = F$

Aplicando o algoritmo de redução, em relação ao operador de **negação**, temos:

	$\neg(\alpha)$	$\neg\neg(\alpha)$
0	1	0
$\frac{1}{2}$	1	0
1	0	1

i) Para $(\alpha = 0) \Rightarrow b(\alpha) = F$

$b(\alpha) = F; b(\neg\alpha) = V; b(\neg(\neg\alpha)) = F.$

ii) Para $\left(\alpha = \frac{1}{2}\right) \Rightarrow b(\alpha) = V.$

$b(\alpha) = V; b(\neg\alpha) = V; b(\neg(\neg\alpha)) = F.$

iii) Para $(\alpha = 1) \Rightarrow b(\alpha) = V.$

$b(\alpha) = V; b(\neg\alpha) = F; b(\neg(\neg\alpha)) = V.$

Em relação ao operador **condicional**, verificamos que o mesmo se comporta de modo clássico, somente com a ressalva de que tanto o valor 1 quanto o $\frac{1}{2}$ estão no conjunto dos valores distinguidos e, diante disso, $v(\frac{1}{2} \to 0) = v(1 \to 0) = 0$. Assim, temos as seguintes cláusulas para o condicional:

iv) $b(\alpha) = F \vee b(\beta) = V \Rightarrow b(\alpha \to \beta) = V, b(\neg(\alpha \to \beta)) = F$

v) $b(\alpha) = V, b(\beta) = F \Rightarrow b(\alpha \to \beta) = F.$

A partir deste ponto, temos condições de extrair as cláusulas que nortearão as bivalorações. Analisemos, novamente, a tabela de valoração para a negação:

	$\neg(\alpha)$	$\neg\neg(\alpha)$
0	1	0
$\frac{1}{2}$	1	0
1	0	1

Quando olhamos para os valores de verdade da negação simples, verificamos que a única conclusão que podemos tirar é que:

$$b(\neg\alpha) = F \Rightarrow b(\alpha) = V.$$

Pois, se $b(\neg\alpha) = V$, não temos como afirmar o valor de $b(\alpha)$ já que: $b(\neg\alpha) = V \Rightarrow b(\alpha) = F$ ou $b(\alpha) = V$.
Portanto:

$$b(\neg\alpha) = F \Rightarrow b(\alpha) = V \text{ (1ªcláusula).}$$

Em relação à dupla negação, concluímos que:

$$b(\neg\neg\alpha) = V \Rightarrow b(\neg\alpha) = F.$$

Do mesmo modo que o caso anterior, nada podemos afirmar a respeito de $b(\neg\neg\alpha) = F$, pois: $b(\neg\neg\alpha) = F \Rightarrow b(\neg\alpha) = V$, para $b(\alpha) = F$ e $b(\alpha) = V$.

Portanto:

$$b(\neg\neg\alpha) = V \Rightarrow b(\neg\alpha) = F \text{ (2ªcláusula)}.$$

As demais cláusulas são consequências do operador condicional, o qual comporta-se classicamente. Resumidamente temos:

1. $b(\neg\alpha) = F \Rightarrow b(\alpha) = V$.
2. $b(\neg\neg\alpha) = V \Rightarrow b(\neg\alpha) = F$
3. $b(\alpha \to \beta) = V \Rightarrow b(\alpha) = F \vee b(\beta) = V$
4. $b(\alpha \to \beta) = F \Rightarrow b(\alpha) = V, b(\beta) = F$
5. $b(\neg(\alpha \to \beta)) = V \Rightarrow b(\alpha) = V, b(\beta) = F$

Os axiomas (1)- (5), adicionados com as propriedades de consequência, C1 e C2 abaixo, caracterizam a semântica diádica para P_3^1.
(C1): $\top \Rightarrow b(\alpha) = V$ ou $b(\alpha) = F$.
(C2): $b(\alpha) = V, b(\alpha) = F \Rightarrow \perp$.

Exemplo 4.2.10. A Lógica Paraconsistente P_4^1.

A lógica P_4^1 foi introduzida em (Carnielli & Marcos 1999) e (Carnielli & Lima-Marques 1999), constituída por: $P_4^1 = \left\langle \left\{0, \frac{1}{3}, \frac{2}{3}, 1\right\}, \{\neg, \to\}, \left\{\frac{1}{3}, \frac{2}{3}, 1\right\rangle\right\}$. Enfatizando o fato de que os valores distinguidos são $\mathcal{D} = \left\{\frac{1}{3}, \frac{2}{3}, 1\right\}$, eis as seguintes matrizes de valores de verdades dos conectivos do sistema:

	$\neg$
0	1
$\frac{1}{3}$	$\frac{2}{3}$
$\frac{2}{3}$	1
1	0

$\to$	0	$\frac{1}{3}$	$\frac{2}{3}$	1
0	1	1	1	1
$\frac{1}{3}$	0	1	1	1
$\frac{2}{3}$	0	1	1	1
1	0	1	1	1

A análise deve ser realizada, assim como no exemplo anterior, em relação à negação, pois ela separa os valores de verdade, tais como:

$$v(0) = 1 \neq \tfrac{2}{3} = v(\tfrac{1}{3})$$
$$v(\tfrac{1}{3}) = \tfrac{2}{3} \neq 1 = v(\tfrac{2}{3})$$

Segue que:

	$\neg$	$\neg\neg$
0	1	0
$\frac{1}{3}$	$\frac{2}{3}$	1
$\frac{2}{3}$	1	0
1	0	1

i) Para $(\alpha = 0) \Rightarrow b(\alpha) = F$.
$b(\alpha) = F; b(\neg\alpha) = V; b(\neg(\neg\alpha)) = F$.

ii) Para $(\alpha = 1/3) \Rightarrow b(\alpha) = V$.
$b(\alpha) = V; b(\neg\alpha) = V; b(\neg(\neg\alpha)) = V$.

iii) Para $(\alpha = 2/3) \Rightarrow b(\alpha) = V$.
$b(\alpha) = V; b(\neg\alpha) = V; b(\neg(\neg\alpha)) = F$.

iv) Para $(\alpha = 1) \Rightarrow b(\alpha) = V$.
$b(\alpha) = V; b(\neg\alpha) = F; b(\neg(\neg\alpha)) = V$.

A partir dos resultados acima, e aplicando a LPO, temos as seguintes cláusulas da bivaloração:

1. $b(\neg\alpha) = F \Rightarrow b(\alpha) = V$.
2. $b(\neg\neg\alpha) = V \Rightarrow b(\alpha) = V$.
3. $b(\neg\neg\neg\alpha) = V \Rightarrow b(\neg\neg\alpha) = F$.

A implicação é clássica e, portanto, são válidas as cláusulas apresentadas no exemplo anterior. Logo, os axiomas abaixo, mais as propriedades (C1) e (C2) caracterizam uma semântica diádica para P_4^1.

1. $b(\neg\alpha) = F \Rightarrow b(\alpha) = V$.
2. $b(\neg\neg\alpha) = V \Rightarrow b(\alpha) = V$.
3. $b(\neg\neg\neg\alpha) = V \Rightarrow b(\neg\neg\alpha) = F$.
4. $b(\alpha \to \beta) = V \Rightarrow b(\alpha) = F \vee b(\beta) = V$
5. $b(\alpha \to \beta) = F \Rightarrow b(\alpha) = V, b(\beta) = F$
6. $b(\neg(\alpha \to \beta)) = V \Rightarrow b(\alpha) = V, b(\beta) = F$

Exemplo 4.2.11. A Lógica Paraconsistente LFI1.

Como nos dois casos anteriores o conectivo da negação foi o separador dos valores de verdade, neste exemplo utilizaremos um outro operador, $\bullet$. Consideremos a lógica proposicional paraconsistente:
$LFI1 = \left\langle \left\{0, \frac{1}{2}, 1\right\}, \{\neg, \bullet, \to, \wedge, \vee\}, \left\{\frac{1}{2}, 1\right\}\right\rangle$, cujas matrizes são:

	$\neg$	$\bullet$	$\circ$
0	1	0	1
$\frac{1}{2}$	$\frac{1}{2}$	1	0
1	0	0	1

$\Rightarrow$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	0	$\frac{1}{2}$	1
1	0	$\frac{1}{2}$	1

Claramente, $\bullet p$ separa $\frac{1}{2}$ e 1 e $\neg p$ separa $\frac{1}{2}$ e 1. O condicional comporta-se como o clássico, sendo necessário apenas ressaltar que $\frac{1}{2}$ está no conjunto dos valores distinguidos.
Analisando $\bullet$ e a negação temos:
a) $x = 0 \Rightarrow b(\alpha) = F, b(\neg\alpha) = V, b(\bullet\alpha) = F, b(\circ\alpha) = V$
b) $x = 1/2 \Rightarrow b(\alpha) = V, b(\neg\alpha) = V, b(\bullet\alpha) = V, b(\circ\alpha) = F$
c) $x = 1 \Rightarrow b(\alpha) = V, b(\neg\alpha) = F, b(\bullet\alpha) = F, b(\circ\alpha) = V$

Aplicando regras da LPO, temos as seguintes cláusulas da bivaloração:

1. $b(\neg\alpha) = V \Rightarrow (b(\alpha) = F)$ ou $(b(\bullet\alpha) = V)$;
2. $b(\neg\alpha) = F \Rightarrow b(\alpha) = V, b(\bullet\alpha) = F$;
3. $b(\bullet\alpha) = V \Rightarrow b(\alpha) = V$;
4. $b(\bullet \bullet \alpha) = V \Rightarrow b(\bullet\alpha) = F$;
5. $b(\bullet\neg\alpha) = V \Rightarrow b(\bullet\alpha) = V$;
6. $b(\bullet\neg\alpha) = F \Rightarrow (b(\neg\alpha) = F)$ ou $(b(\alpha) = F)$.

Os demais operadores comportam-se classicamente. Os axiomas acima munidos das propriedades (C1) e (C2) consitituem uma semântica diádica para **LFI1**.

Exemplo 4.2.12. A Lógica 4-valorada de Belnap.
A lógica paraconsistente de Belnap,
$B = \left\langle \left\{0, \frac{1}{3}, \frac{2}{3}, 1\right\}, \{\neg, \wedge, \vee\}, \left\{\frac{2}{3}, 1\right\}\right\rangle$, pode ser representada pelas seguintes matrizes:

	$\neg$
0	0
$\frac{1}{3}$	$\frac{2}{3}$
$\frac{2}{3}$	$\frac{1}{3}$
1	1

$\wedge$	0	$\frac{1}{3}$	$\frac{2}{3}$	1
0	0	0	0	0
$\frac{1}{3}$	0	$\frac{1}{3}$	0	$\frac{1}{3}$
$\frac{2}{3}$	0	0	$\frac{2}{3}$	$\frac{2}{3}$
1	0	$\frac{1}{3}$	$\frac{2}{3}$	1

$\vee$	0	$\frac{1}{3}$	$\frac{2}{3}$	1
0	0	$\frac{1}{3}$	$\frac{2}{3}$	1
$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	1	1
$\frac{2}{3}$	$\frac{2}{3}$	1	$\frac{2}{3}$	1
1	1	1	1	1

Claramente, $\neg p$ separa 1 e $\frac{2}{3}$ e $\frac{1}{3}$ e 1. Assim:
i) $x = 0 \Rightarrow b(\alpha) = F, b(\neg\alpha) = F$;
ii) $x = \frac{1}{2} \Rightarrow b(\alpha) = F, b(\neg\alpha) = V$;
iii) $x = \frac{2}{3} \Rightarrow b(\alpha) = V, b(\neg\alpha) = F$;
iv) $x = 1 \Rightarrow b(\alpha) = V, b(\neg\alpha) = V$.

A partir da tabela da negação e usando a LPO, obtemos as seguintes cláusulas da bivaloração:

1. $b(\neg\neg\alpha) = V \rightarrow b(\alpha) = V$;
2. $b(\neg\neg\alpha) = F \rightarrow b(\alpha) = F$.

Os demais operadores comportam-se classicamente. Os axiomas acima juntamente com C1 e C2, dão-nos uma semântica diádica para B_4.

4.3 Anéis de Polinômios e a Tese de Suszko

Nesta seção, apresentaremos os anéis de polinômios para cada um dos sistemas que foram reduzimos em uma semântica bivalente.

4.3.1 Um cálculo de Anel de Polinômios em $\mathbb{Z}_2[X \cup X']$ para a Lógica Paraconsistente $\mathbf{P}_3^1$

A lógica $\mathbf{P}_3^1$ é constituída por $\mathbf{P}_3^1 = \langle \{0, \frac{1}{2}, 1\}, \{\neg, \rightarrow\}, \{\frac{1}{2}, 1\} \rangle$, tendo as seguintes tabelas de verdade:

	0	$\frac{1}{2}$	1
$\neg$	1	1	0

$\rightarrow$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	0	1	1
1	0	1	1

A fim de tornarmos nossos cálculos mais fáceis, ao invés de trabalharmos com frações, tomaremos uma tabela isomórfica à original por meio da multiplicação de todos os seus valores de verdade pelo número 2, ou seja:

	0	1	2
$\neg$	2	2	0

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

Nosso objetivo agora é, mediante as cláusulas da bivaloração para a lógica $\mathbf{P}_3^1$, desenvolver um polinômio que caracterize tais condições. Apesar de ainda não termos comentado a respeito da perda da verofuncionalidade na redução de Suszko, pois faremos uma seção apenas a respeito deste fato, isso ocorre e o polinômio a ser desenvolvido deve refletir tal característica.

Diante disso, teremos que lançar mão do uso das variáveis ocultas, pois são elas que representarão a perda da verofuncionalidade dos sistemas.

Apresentadas as seguintes cláusulas de bivaloração para o sistema $\mathbf{P}_3^1$,

1. $b(\neg\alpha) = F \Rightarrow b(\alpha) = V$.
2. $b(\neg\neg\alpha) = V \Rightarrow b(\neg\alpha) = F$
3. $b(\alpha \rightarrow \beta) = V \Rightarrow b(\alpha) = F \vee b(\beta) = V$
4. $b(\alpha \rightarrow \beta) = F \Rightarrow b(\alpha) = V, b(\beta) = F$
5. $b(\neg(\alpha \rightarrow \beta)) = V \Rightarrow b(\alpha) = V, b(\beta) = F$

Os polinômios que traduzem estas cláusulas são dados por:

$$(\neg\alpha)^* = \alpha^* \cdot x_\alpha + 1, \text{ onde } x_\alpha \text{ é uma variável oculta.}$$
$$(\neg\neg\alpha)^* = (\alpha^* \cdot x_\alpha + 1) \cdot x_{\neg\alpha} + 1.$$

Restrição: $x_{\neg\alpha} = 1$.

Antes de analisarmos os polinômios apresentados, devemos avaliar o motivo dessa restrição, $x_{\neg\alpha} = 1$. Isso decorre do fato de que a dupla negação é *clássica*, ou seja:

	0	$\frac{1}{2}$	1
$\neg$	1	1	0
$(\neg\neg)$	0	0	1

Assim, considerando $\neg\alpha = \beta$ temos:
$(\neg\neg\alpha)^* = (\neg\beta)^* = \beta^*.x_\beta + 1 = (\neg\alpha)^*.x_\beta + 1 = (\alpha^*.x_\alpha + 1).x_\beta + 1$[1].
$(\neg\neg\alpha)^* = (\alpha^* \cdot x_\alpha + 1) \cdot x_{\neg\alpha} + 1$.

Percebemos que, os polinômios apresentados para a lógica $\mathbf{P}_3^1$ referem-se apenas aos operadores de negação e dupla negação. Ocorre que, como os demais conectivos comportam-se classicamente, as traduções polinomiais apresentadas para o calculo proposicional clássico também são válidas aqui.

Verifiquemos, informalmente, que $(\neg\alpha)^* = \alpha^* \cdot x_\alpha + 1$ e $(\neg\neg\alpha)^* = (\alpha^* \cdot x_\alpha + 1) \cdot x_{\neg\alpha} + 1$, realmente representam as cláusulas da bivaloração para o sistema em questão.
(1ªcláusula) $b(\neg\alpha) = F \Rightarrow b(\alpha) = V$.
Se $b(\neg\alpha) = F$, então:
$(\neg\alpha)^* = 0 \Rightarrow \alpha^* \cdot x_\alpha + 1 = 0 \Rightarrow \alpha^* \cdot x_\alpha = 1 \Rightarrow \alpha^* = 1$ e $x_\alpha = 1$.
De fato, o polinômio para a negação satisfaz essa cláusula.

(2ªcláusula) $b(\neg\neg\alpha) = V \Rightarrow b(\neg\alpha) = F$.
$b(\neg\neg\alpha) = V \Rightarrow (\neg\neg\alpha)^* = 1 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_{\neg\alpha} + 1 = 1 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_{\neg\alpha} = 0 \Rightarrow x_{\neg\alpha} = 0$ ou $(\alpha^* \cdot x_\alpha + 1) = 0$. Como, pela restrição $x_{\neg\alpha} = 1$, então a primeira possibilidade não se aplica. Da segunda parte da conclusão, $(\alpha^* \cdot x_\alpha + 1) = 0$ temos que $(\neg\alpha)^* = 0$.

Essas observações são, conforme já dissemos, "intuitivas". A fim de provarmos que de fato esses polinômios satisfazem as cláusulas, apresentamos o seguinte teorema.

Teorema 4.3.1. *Para a lógica paraconsistente trivalorada P_3^1, as seguintes condições são equivalentes:*
(i) A lógica paraconsistente P_3^1 é caracterizada por uma semântica bivalorada definida pelas seguintes cláusulas:

1. $b(\neg\alpha) = F \rightarrow b(\alpha) = V$;
2. $b(\neg\neg\alpha) = V \rightarrow b(\neg\alpha) = F$;
3. $b(\alpha \Rightarrow \beta) = V \rightarrow b(\alpha) = F \mid b(\beta) = V$;
4. $b(\alpha \Rightarrow \beta) = F \rightarrow b(\alpha) = V, b(\beta) = F$;
5. $b(\neg(\alpha \Rightarrow \beta)) = V \rightarrow b(\alpha) = V, b(\beta) = F$.

[1]Neste capítulo, e no capítulo 5, omitiremos a notação de interpretação $I : \mathbb{Z}_2[X \cup X'] \rightarrow \mathbb{Z}_2$

C1: $\top \rightarrow b(\alpha) = V \mid b(\alpha) = F$*;*
C2: $b(\alpha) = V, b(\alpha) = F \rightarrow \perp$*; para todo* $\alpha \in \mathcal{S}$*, onde* $\mathcal{S}$ *denota um conjunto não-vazio de fórmulas.*
(ii) A tradução polinomial a respeito da semântica diádica para P_3^1 *é finita e representa o sistema* P_3^1*.*

Demonstração: $(i) \Rightarrow (ii)$
Os polinômios em questão são:
$(\neg\alpha)^* = \alpha^* \cdot x_\alpha + 1$, onde x_α é uma variável oculta.
$(\neg\neg\alpha)^* = (\alpha^* \cdot x_\alpha + 1) \cdot x_{\neg\alpha} + 1$.
$(\alpha \Rightarrow \beta) = \alpha^*\beta^* + \alpha^* + 1$.

Restrição: $x_{\neg\alpha} = 1$.
Portanto, a tradução a respeito da semântica diádica para P_3^1 é finita. Agora provaremos que, de fato, ela representa o sistema P_3^1.

(1ªcláusula) $b(\neg\alpha) = F \rightarrow b(\alpha) = V$.

$b(\neg\alpha) = 0 \Rightarrow \alpha^* \cdot x_\alpha + 1 = 0$. Logo, $\alpha^* \cdot x_\alpha = 1 \Rightarrow (\alpha^* = 1)$ e $(x_\alpha = 1)$.
$\therefore b(\neg\alpha) = F \Rightarrow b(\alpha) = V$.

(2ªcláusula) $b(\neg\neg\alpha) = V \rightarrow b(\neg\alpha) = F$;

$b(\neg\neg\alpha) = 1 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_{\neg\alpha} + 1 = 1 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_{\neg\alpha} = 0$. Logo, $x_{\neg\alpha} = 0$ ou $(\alpha^* \cdot x_\alpha + 1) = 0 \Rightarrow b(\neg\alpha) = 0$.
$\therefore b(\neg\neg\alpha) = V \rightarrow b(\neg\alpha) = F$.

$(ii) \Rightarrow (i)$

1ºcaso: $b(\neg\alpha) = 1, b(\neg\alpha) = 0$

(a) $\alpha^* \cdot x_\alpha + 1 = 1 \Rightarrow \alpha^* \cdot x_\alpha = 0$. Então, $\alpha^* = 0$ ou $x_\alpha = 0$. Logo, se $x_\alpha = 0$, então $b(\alpha) = 1$ ou $b(\alpha) = 0$. Isso significa que o valor de α é indeterminado.
$\therefore b(\neg\alpha) = V \Rightarrow b(\alpha) = V$ ou $b(\alpha) = F$
(b) $\alpha^* \cdot x_\alpha + 1 = 0 \Rightarrow \alpha^* \cdot x_\alpha = 1 \Rightarrow (\alpha)^* = 1$.
$\therefore b(\neg\alpha) = F \Rightarrow b(\alpha) = V$.

2ºcaso: $b(\neg\neg\alpha) = 1, b(\neg\neg\alpha) = 0$

(a) $b(\neg\neg\alpha) = 1 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_{\neg\alpha} + 1 = 1 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_{\neg\alpha} = 0 \Rightarrow x_{\neg\alpha} = 0$ ou $\alpha^* \cdot x_\alpha + 1 = 0$, então em decorrência da restrição $x_{\neg\alpha} = 1$, temos $b(\neg\alpha) = 0$.
$\therefore b(\neg\neg\alpha) = V \Rightarrow b(\neg\alpha) = F \Rightarrow b(\alpha) = V$.
(b) $b(\neg\neg\alpha) = 0 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_{\neg\alpha} + 1 = 0 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_{\neg\alpha} = 1 \Rightarrow x_{\neg\alpha} = 1, \alpha^* \cdot x_\alpha + 1 = 1$. Então, $(\alpha)^* = 1$ ou $x_\alpha = 1$.
$\therefore b(\neg\neg\alpha) = F \Rightarrow b(\alpha) = F$ ou $b(\alpha) = V$.

Para o operador condicional não exporemos as demonstrações em razão de seu comportamento clássico. ∎

4.3.2 Um cálculo de Anel de Polinômios para a Lógica Paraconsistente $\mathbf{P}_4^1$

A lógica P_4^1 é constituída por $P_4^1 = \left\langle \left\{0, \frac{1}{3}, \frac{2}{3}, 1\right\}, \{\neg, \Rightarrow\}, \left\{\frac{1}{3}, \frac{2}{3}, 1\right\}\right\rangle$, tendo como tabelas de verdade:

	0	$\frac{1}{3}$	$\frac{2}{3}$	1
$\neg$	1	$\frac{2}{3}$	1	0
$\neg\neg$	0	1	0	1
$\neg\neg\neg$	1	0	1	0

$\rightarrow$	0	$\frac{1}{3}$	$\frac{2}{3}$	1
0	1	1	1	1
$\frac{1}{3}$	0	1	1	1
$\frac{2}{3}$	0	1	1	1
1	0	1	1	1

A partir da matriz de valoração para $(\neg)$, obtemos, após aplicarmos LPO, as seguintes cláusulas para a bivaloração de $\mathbf{P}_4^1$:
(i) $b(\neg\alpha) = F \Rightarrow b(\alpha) = V$;
(ii) $b(\neg\neg\alpha) = V \Rightarrow b(\alpha) = V$;
(iii) $b(\neg\neg\neg\alpha) = V \Rightarrow b(\neg\neg\alpha) = F$.

Os polinômios que satisfazem essas cláusulas são dados por:

- $(\neg\alpha)^* = \alpha^* \cdot x_\alpha + 1$, onde x_α é uma variável oculta.
- $(\neg\neg\alpha)^* = (\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} + 1$.
- $(\neg\neg\neg\alpha)^* = ((\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} + 1) \cdot x_{\alpha'''} + 1$.

Restrição: $x_{\alpha''} = 1$ e $x_{\alpha'''} = 1$.

As restrições são decorrentes do mesmo motivo do caso anterior, ou seja, tanto a dupla negação quanto a tripla negação comportam-se classicamente.

Teorema 4.3.2. *Para a lógica Paraconsistente 4-valorada P_4^1, as seguintes condições são equivalentes:*
(i) A lógica paraconsistente P_4^1 é caracterizada por uma semântica bivalorada definida pelas seguintes cláusulas:

1. $b(\neg\alpha) = F \Rightarrow b(\alpha) = V$.
2. $b(\neg\neg\alpha) = V \Rightarrow b(\alpha) = V$.
3. $b(\neg\neg\neg\alpha) = V \Rightarrow b(\neg\neg\alpha) = F$.
4. $b(\alpha \rightarrow \beta) = V \Rightarrow b(\alpha) = F \vee b(\beta) = V$
5. $b(\alpha \rightarrow \beta) = F \Rightarrow b(\alpha) = V, b(\beta) = F$
6. $b(\neg(\alpha \rightarrow \beta)) = V \Rightarrow b(\alpha) = V, b(\beta) = F$
   C1: $\top \rightarrow b(\alpha) = V \mid b(\alpha) = F$;
   C2: $b(\alpha) = V, b(\alpha) = F \rightarrow \bot$; *para todo $\alpha \in \mathcal{S}$, onde $\mathcal{S}$ denota um conjunto não-vazio de fórmulas.*

(ii) A tradução polinomial a respeito da semântica diádica para P_4^1 é finita e representa o sistema P_4^1.

Demonstração:

$(i) \Rightarrow (ii)$

Os polinômios em questão são:

- $(\neg\alpha)^* = \alpha^* \cdot x_\alpha + 1$, onde x_α é uma variável oculta.
- $(\neg\neg\alpha)^* = (\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} + 1$.
- $(\neg\neg\neg\alpha)^* = ((\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} + 1) \cdot x_{\alpha'''} + 1$.
- $(\alpha \Rightarrow \beta) = \alpha^*\beta^* + \alpha^* + 1$.

Restrição: $x_{\alpha''} = 1$ e $x_{\alpha'''} = 1$.

Portanto, a tradução a respeito da semântica diádica para P_4^1 é finita. Agora provaremos que, de fato, ela representa o sistema P_4^1.

(1ªcláusula) $b(\neg\alpha) = F \Rightarrow b(\alpha) = V$; $b(\neg\alpha) = 0 \Rightarrow \alpha^* \cdot x_\alpha + 1 = 0$. Logo, $\alpha^* \cdot x_\alpha = 1 \Rightarrow (\alpha^* = 1)$ e $(x_\alpha = 1)$.
$\therefore b(\neg\alpha) = F \Rightarrow b(\alpha) = V$.

(2ªcláusula) $b(\neg\neg\alpha) = V \Rightarrow b(\alpha) = V$;

$b(\neg\neg\alpha) = 1 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} + 1 = 1 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} = 0$. Logo, $(x_{\alpha''} = 0)$ ou $(\alpha^* \cdot x_\alpha + 1) = 0 \Rightarrow b(\alpha) = 1$. A cláusula $x_{\alpha''} = 0$ não pode ocorrer devido a restrição.
$\therefore b(\neg\neg\alpha) = V \Rightarrow b(\alpha) = V$.

(3ªcláusula) $b(\neg\neg\neg\alpha) = V \Rightarrow b(\neg\neg\alpha) = F$;

$b(\neg\neg\alpha) = 1 \Rightarrow ((\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} + 1) \cdot x_{\alpha'''} + 1 = 1 \Rightarrow ((\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} + 1) \cdot x_{\alpha'''} = 0$. Logo, $(x_{\alpha'''} = 0)$ ou $((\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} + 1) = 0 \Rightarrow b(\neg\neg\alpha) = 0$.
$\therefore b(\neg\neg\neg\alpha) = V \Rightarrow b(\neg\neg\alpha) = F$.

$(ii) \Rightarrow (i)$

1ºcaso: $b(\neg\alpha) = 0, b(\neg\alpha) = 1$

(a) $b(\neg\alpha) = 0$, já demonstrado.

(b) $b(\neg\alpha) = 1 \Rightarrow \alpha^* \cdot x_\alpha + 1 = 1 \Rightarrow \alpha^* \cdot x_\alpha = 0 \Rightarrow ((\alpha)^* = 0)$ ou $(x_\alpha = 0)$. Isso significa que, $b(\alpha) = 1$ ou $b(\alpha) = 0$, o valor de α é indeterminado, e consequentemente, $b(\neg\alpha)$ também o é.

2ºcaso: $b(\neg\neg\alpha) = 1, b(\neg\neg\alpha) = 0$

(a) $b(\neg\neg\alpha) = 1$, já demonstrado.

(b) $b(\neg\neg\alpha) = 0 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} + 1 = 0 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} = 1 \Rightarrow (x_{\alpha''} = 1)$ e $(\alpha^* \cdot x_\alpha + 1) = 1 \Rightarrow (\alpha^* \cdot x_\alpha = 0) \Rightarrow (\alpha^* = 0)$ ou $(x_\alpha = 0)$. Isso significa que o valor de α é indeterminado.

3ºcaso: $b(\neg\neg\neg\alpha) = 1, b(\neg\neg\neg\alpha) = 0$

(a) $b(\neg\neg\neg\alpha) = 1$, já demonstrado.
(b) $b(\neg\neg\neg\alpha) = 0 \Rightarrow ((\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} + 1) \cdot x_{\alpha'''} + 1 = 0 \Rightarrow (x_{\alpha'''} = 1), ((\alpha^* \cdot x_\alpha + 1) \cdot x_{\alpha''} + 1) = 1 \Rightarrow b(\neg\neg\alpha) = 1 \Rightarrow b(\alpha) = 1.$ ■

4.3.3 Um Anel de polinômio para a Lógica Paraconsistente LFI1

A lógica paraconsistente **LFI1** é formada por:
LFI1 $= \left\langle \left\{0, \frac{1}{2}, 1\right\}, \{\neg, \circ, \Rightarrow, \wedge, \vee\}, \left\{\frac{1}{2}, 1\right\}\right\rangle$, tendo como matrizes de valorações as seguintes tabelas:

	0	$\frac{1}{2}$	1
$\neg$	1	$\frac{1}{2}$	0
$\circ$	1	0	1
$\bullet$	0	1	0
$\circ\circ$	1	1	1
$\bullet\bullet$	0	0	0
$\bullet\neg$	0	1	0
$\circ\neg$	1	0	1

$\Rightarrow$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	0	$\frac{1}{2}$	1
1	0	$\frac{1}{2}$	1

A partir das tabelas de verdade para os operadores $(\neg)$ e $(\circ)$, obtemos, após aplicarmos a LPO, as seguintes cláusulas para a bivaloração de **LFI1**:

(i) $b(\neg\alpha) = V \rightarrow b(\alpha) = F \mid b(\circ\alpha) = F$;

(ii) $b(\neg\alpha) = F \rightarrow b(\alpha) = V, b(\circ\alpha) = V$;

(iii) $b(\circ\alpha) = F \rightarrow b(\neg\alpha) = V$

(iv) $b(\circ \circ \alpha) = F \rightarrow b(\circ\alpha) = V$

(v) $b(\circ\neg\alpha) = F \rightarrow b(\circ\alpha) = F$

(vi)$b(\circ\neg\alpha) = V \rightarrow b(\neg\alpha) = F \mid b(\alpha) = F$

Os polinômios que satisfazem essas cláusulas são dados por:

- $(\neg\alpha)^* = \alpha^* \cdot x_\alpha + 1$, onde x_α é uma variável oculta.
- $(\circ\alpha)^* = (\alpha^* \cdot (x_\alpha + 1) + 1)\, x_\alpha$.
- $(\circ\neg\alpha)^* = ((\alpha^* \cdot x_\alpha + 1) \cdot (x_\alpha + 1) + 1)\, x_\alpha$.
- $(\circ \circ \alpha)^* = (((\alpha^* \cdot (x_\alpha + 1) + 1).x_\alpha) \cdot (x_\alpha + 1) + 1)\, x_\alpha$.
  Restrição: $x_\alpha = 1$.

Observação 4.3.3. A lógica paraconsistente LFI1, em sua apresentação clássica, possui dois axiomas referentes à dupla negação, que na maioria das LFIs não são validados. São eles:
(cf)$\neg\neg\alpha \rightarrow \alpha$.
(ce) $\alpha \rightarrow \neg\neg\alpha$.
Decorre que, em função disso e da propriedade da comutatividade, $\circ \circ \alpha = \top$. Para que nosso polinômio atenda a essas características, precisamos que a variável oculpa x_α assuma valor 1.

Teorema 4.3.4. *Para a lógica Paraconsistente **LFI1**, as seguintes condições são equivalentes:*
*(i) A lógica paraconsistente **LFI1** é caracterizada por uma semântica bivalorada definida pelas seguintes cláusulas:*

1. $b(\neg\alpha) = V \Rightarrow b(\alpha) = F$ *ou* $b(\circ\alpha) = F$;
2. $b(\neg\alpha) = F \Rightarrow b(\alpha) = V$ *e* $b(\circ\alpha) = V$;
3. $b(\circ\alpha) = F \Rightarrow b(\neg\alpha) = V$;
4. $b(\circ \circ \alpha) = F \Rightarrow b(\circ\alpha) = V$;
5. $b(\circ\neg\alpha) = F \Rightarrow b(\circ\alpha) = F$;
6. $b(\circ\neg\alpha) = V \Rightarrow b(\neg\alpha) = F$ *ou* $b(\alpha) = F$.
   C1: $\top \Rightarrow b(\alpha) = V$ *ou* $b(\alpha) = F$;
   C2: $b(\alpha) = V, b(\alpha) = F \Rightarrow \bot$; *para todo* $\alpha \in \mathcal{S}$, *onde* $\mathcal{S}$ *denota um conjunto não-vazio de fórmulas.*

*(ii) A tradução polinomial a respeito da semântica diádica para **LFI1** é finita e representa o sistema **LFI1**.*

Demonstração: $(i) \Rightarrow (ii)$
Os polinômios em questão são:

- $(\neg\alpha)^* = \alpha^* \cdot x_\alpha + 1$, onde x_α é uma variável oculta.
- $(\circ\alpha)^* = (\alpha^* \cdot (x_\alpha + 1) + 1)\, x_\alpha$.
- $(\circ\neg\alpha)^* = ((\alpha^* \cdot x_\alpha + 1) \cdot (x_\alpha + 1) + 1)\, x_\alpha$.
- $(\circ \circ \alpha)^* = (((\alpha^* \cdot (x_\alpha + 1) + 1).x_\alpha) \cdot (x_\alpha + 1) + 1)\, x_\alpha$.
  Restrição: $x_\alpha = 1$.

- $(\alpha \Rightarrow \beta) = \alpha^*\beta^* + \alpha^* + 1$.

Portanto, a tradução a respeito da semântica diádica para **LFI1** é finita. Agora provaremos que, de fato, ela representa o sistema **LFI1**.

1ªcláusula: $b(\neg\alpha) = V \Rightarrow b(\alpha) = F$ ou $b(\circ\alpha) = F$;
$b(\neg\alpha) = 1 \Rightarrow \alpha^* \cdot x_\alpha + 1 = 1$. Logo, $\alpha^* \cdot x_\alpha = 0 \Rightarrow (\alpha^* = 0)$ ou $(x_\alpha = 0)$.

- Se $(\alpha^* = 0)$, então a primeira condição está satisfeita, ou seja, $b(\alpha) = F$.
- Se $(x_\alpha = 0)$, então:
  $b(\circ\alpha) = (\alpha^* \cdot (x_\alpha + 1) + 1)\, x_\alpha \Rightarrow (\alpha^* \cdot (x_\alpha + 1) + 1)\, .0 = 0 \Rightarrow b(\circ\alpha) = 0$.

Logo, $b(\neg\alpha) = V \Rightarrow b(\alpha) = F$ ou $b(\circ\alpha) = F$.

2ªcláusula: $b(\neg\alpha) = F \Rightarrow b(\alpha) = V$ e $b(\circ\alpha) = V$;
$b(\neg\alpha) = F \Rightarrow (\alpha)^* \cdot x_\alpha + 1 = 0 \Rightarrow (\alpha)^* \cdot x_\alpha = 1 \Leftrightarrow (\alpha)^* = 1$ e $x_\alpha = 1$.
Como $x_\alpha = 1$, então:
$b(\circ\alpha) = \alpha^*(x_\alpha + 1) + 1 \Rightarrow \alpha^*(1 + 1) + 1 \Rightarrow b(\circ\alpha) = 1$.
Portanto, $b(\neg\alpha) = F \Rightarrow b(\alpha) = V$ e $b(\circ\alpha) = V$.

3ªcláusula: $b(\circ\alpha) = F \Rightarrow b(\neg\alpha) = V$.
$b(\circ\alpha) = (\alpha^*(x_\alpha + 1) + 1)\, x_\alpha = 0 \Rightarrow (x_\alpha = 0)$ ou $((\alpha^*(x_\alpha + 1) + 1) = 0) \Rightarrow \alpha^*(x_\alpha + 1) = 1 \Rightarrow (\alpha^* = 1)$ e $x_\alpha = 0$. Assim, temos a seguinte possibilidade: $(x_\alpha = 0)$ ou $(\alpha^* = 1, x_\alpha = 0)$. Isto é, necessariamente $x_\alpha = 0$. Então, $b(\neg\alpha) = \alpha^*.x_\alpha + 1 = 0 + 1 = 1$. Portanto, $b(\neg\alpha) = V$.

4ªcláusula: $b(\circ\circ\alpha) = F \Rightarrow b(\circ\alpha) = V$;
$b(\circ\circ\alpha) = (((\alpha^* \cdot (x_\alpha + 1) + 1).x_\alpha) \cdot (x_\alpha + 1) + 1)\, x_\alpha = 0$
$\Rightarrow (x_\alpha = 0)$ ou $(((\alpha^* \cdot (x_\alpha + 1) + 1).x_\alpha) \cdot (x_\alpha + 1) + 1) = 0 \Rightarrow (((\alpha^* \cdot (x_\alpha + 1) + 1).x_\alpha) \cdot (x_\alpha + 1) = 1 \Rightarrow (((\alpha^* \cdot (x_\alpha + 1) + 1).x_\alpha) = 1$ e $(x_\alpha + 1) = 1$.
Se $(\alpha^* \cdot (x_\alpha + 1) + 1).x_\alpha = 1 \Rightarrow b(\circ\alpha) = 1$.
Os outros dois casos referem-se ao valor de x_α que assume valor falso. No entanto, em virtude da restrição, tal situação não é válida. Portanto:
$b(\circ\circ\alpha) = F \Rightarrow b(\circ\alpha) = V$.

5ªcláusula: $b(\circ\neg\alpha) = F \Rightarrow b(\circ\alpha) = F$;
$(\circ\neg\alpha)^* = ((\alpha^* \cdot x_\alpha + 1) \cdot (x_\alpha + 1) + 1)\, x_\alpha = 0 \Rightarrow (x_\alpha = 0)$ ou $((\alpha^* \cdot x_\alpha + 1) \cdot (x_\alpha + 1) + 1) = 0$.
Se $((\alpha^* \cdot x_\alpha + 1) \cdot (x_\alpha + 1) + 1) = 0 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot (x_\alpha + 1) = 1 \Rightarrow (x_\alpha = 0)$ e $((\alpha^* = 0)$ ou $(x_\alpha = 0))$. Diante disso, temos as seguintes possibilidades: (a) $x_\alpha = 0$
(b) $(x_\alpha = 0)$ e $(\alpha^* = 0)$.
(c) $(x_\alpha = 0)$ e $(x_\alpha = 0)$.
Para todas as possibilidades, $b(\circ\alpha) = F$, pois $b(\circ\alpha) = (\alpha^*(x_\alpha + 1) + 1)\, x_\alpha$ e $x_\alpha = 0$. Logo, $b(\circ\neg\alpha) = F \Rightarrow b(\circ\alpha) = F$.

6ªcláusula: $b(\circ\neg\alpha) = V \Rightarrow b(\neg\alpha) = F$ ou $b(\alpha) = F$;
$(\circ\neg\alpha)^* = ((\alpha^* \cdot x_\alpha + 1) \cdot (x_\alpha + 1) + 1)\, x_\alpha = 1 \Rightarrow (x_\alpha = 1)$ e $(\alpha^* \cdot x_\alpha + 1) \cdot (x_\alpha + 1) + 1 = 1 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot (x_\alpha + 1) = 0 \Rightarrow (x_\alpha + 1)$ ou $(\alpha^* \cdot x_\alpha + 1) = 0$.
Para $(x_\alpha + 1) = 0 \Rightarrow x_\alpha = 1$.
Para $(\alpha^* \cdot x_\alpha + 1) = 0 \Rightarrow (\alpha^* = 1)$ e $x_\alpha = 1$.
Diante disso, temos as seguintes possibilidades de valorações:
(a) $(x_\alpha = 1)$ e $(x_\alpha = 1)$.
Nesta situação, temos:
$b(\circ\alpha) = (\alpha^*(x_\alpha + 1) + 1)\, x_\alpha = (\alpha^*(1 + 1) + 1)\, .1 = 1$. Logo, $b(\circ\alpha) = 1$. Se $b(\circ\alpha) = 1 \Rightarrow (b(\neg\alpha) = 0)$ ou $(b(\alpha) = 0)$, fato este que provaremos na próxima parte da demonstração. Logo,$b(\neg\alpha) = F$ ou $b(\alpha) = F$.
(b) $(x_\alpha = 1)$ e $(\alpha^* = 1)$. Temos que:
$b(\neg\alpha) = 1.1 + 1 = 0$. Portanto, $b(\neg\alpha) = F$.

$(ii) \Rightarrow (i)$

1ºcaso: $b(\neg\alpha) = 0, b(\neg\alpha) = 1$
Ambos já foram demonstrados, pois referem-se à 1ªe 2ªcláusulas das bivalorações.

2ºcaso: $b(\circ\alpha) = 0, b(\circ\alpha) = 1$
(a) $b(\circ\alpha) = 0$, já demonstrado.

(b)$b(\circ\alpha) = 1$.
$(\circ\alpha)^* = (\alpha^* \cdot (x_\alpha + 1) + 1)\, x_\alpha = 1 \Rightarrow (x_\alpha = 1)$ e $(\alpha^* \cdot (x_\alpha + 1) + 1) = 1 \Rightarrow \alpha^* \cdot (x_\alpha + 1) = 0 \Rightarrow (\alpha^* = 0)$ ou $x_\alpha = 1$. Assim, temos que, necessariamente, $x_\alpha = 1$. Se $x_\alpha = 1$, então, $b(\neg\alpha) = \alpha^*.x_\alpha + 1 = 0$. Portanto, $b(\neg\alpha) = \alpha^* + 1$.
Logo, como o valor de $b(\neg\alpha)$ depende do valor de α, tanto os valores de $b(\neg\alpha)$ quanto os de α são indeterminados.

3ºcaso: $b(\circ\circ\alpha) = 0, b(\circ\circ\alpha) = 1$
(a) $b(\circ\circ\alpha) = 0$, já demonstrado.
(b) $b(\circ\circ\alpha) = 1$.
Devemos provar que: $b(\circ\circ\alpha) = F \Rightarrow b(\circ\alpha) = T$.
$(\circ\circ\alpha)^* = (((\alpha^* \cdot (x_\alpha + 1) + 1).x_\alpha) \cdot (x_\alpha + 1) + 1)\, x_\alpha = 0$

4ºcaso: $b(\neg\circ\alpha) = 0, b(\neg\circ\alpha) = 1$.
Ambos já demonstrados. São as cláusulas 5 e 6 da bivaloração. ∎

4.3.4 Um Anel de polinômio para a lógica 4-valorada de Belnap

A lógica paraconsistente $B_4 = \left\langle \left\{0, \frac{1}{3}, \frac{2}{3}, 1\right\}, \{\neg, \wedge, \vee\}, \left\{\frac{2}{3}, 1\right\}\right\rangle$ tem as seguintes tabelas de verdade:

	0	$\frac{1}{3}$	$\frac{2}{3}$	1
$\neg$	0	$\frac{2}{3}$	$\frac{1}{3}$	1
$\neg\neg$	0	$\frac{1}{3}$	$\frac{2}{3}$	1

$\wedge$	0	$\frac{1}{3}$	$\frac{2}{3}$	1
0	0	0	0	0
$\frac{1}{3}$	0	$\frac{1}{3}$	0	$\frac{1}{3}$
$\frac{2}{3}$	0	0	$\frac{2}{3}$	$\frac{2}{3}$
1	0	$\frac{1}{3}$	$\frac{2}{3}$	1

$\vee$	0	$\frac{1}{3}$	$\frac{2}{3}$	1
0	0	$\frac{1}{3}$	$\frac{2}{3}$	1
$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	1	1
$\frac{2}{3}$	$\frac{2}{3}$	1	$\frac{2}{3}$	1
1	1	1	1	1

A partir da tabela de verdade para a negação obtemos, aplicando a LPO, as seguintes cláusulas para a bivaloração da lógica de Belnap:
(i) $b(\neg\neg\alpha) = V \rightarrow b(\alpha) = V$;
(ii) $b(\neg\neg\alpha) = F \rightarrow b(\alpha) = F$.

O polinômio associado às cláusulas da bivaloração é dado por:
$(\neg\neg\alpha)^* = (\alpha^* \cdot x_\alpha + 1) \cdot x_\alpha + 1$.
Restrição: $x_\alpha = 1$.

Teorema 4.3.5. *Para a lógica Paraconsistente 4-valorada B_4, as seguintes condições são equivalentes:*
(i) A lógica paraconsistente B_4 é caracterizada por uma semântica bivalorada definida pelas seguintes cláusulas:

1. $b(\neg\neg\alpha) = V \rightarrow b(\alpha) = V$;
2. $b(\neg\neg\alpha) = F \rightarrow b(\alpha) = F$.

C1: $\top \rightarrow b(\alpha) = V \mid b(\alpha) = F$;
C2: $b(\alpha) = V, b(\alpha) = F \rightarrow \perp$; *para todo $\alpha \in \mathcal{S}$, onde $\mathcal{S}$ denota um conjunto não-vazio de fórmulas.*
(ii) A tradução polinomial a respeito da semântica diádica para B_4 é finita e representa o sistema B_4.

Demonstração: $(i) \Rightarrow (ii)$
Os polinômios em questão são:
$(\neg\neg\alpha)^* = (\alpha^* \cdot x_\alpha + 1) \cdot x_\alpha + 1$.
$(\alpha \wedge \beta)^* = \alpha^*.\beta^*$.
$(\alpha \vee \beta)^* = \alpha^*\beta^* + \alpha^* + \beta^*$.
Restrição: $x_\alpha = 1$.
Portanto, a tradução a respeito da semântica diádica para B_4 é finita. Agora provaremos que, de fato, ela representa o sistema B_4.

(cláusula (1)) $b(\neg\neg\alpha) = V \rightarrow b(\alpha) = V$;
$(\neg\neg\alpha)^* = (\alpha^* \cdot x_\alpha + 1) \cdot x_\alpha + 1 = 1 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_\alpha = 0 \Rightarrow (x_\alpha = 0)$ ou $\alpha^* \cdot x_\alpha + 1 = 0$.
Se $\alpha^* \cdot x_\alpha + 1 = 0 \Rightarrow \alpha^* \cdot x_\alpha = 1 \Rightarrow x_\alpha = 1$ e $\alpha^* = 1$.
A primeira condição de valor de verdade, $(x_\alpha = 0)$ não é válida, em decorrência da restrição. Da segunda condição, $x_\alpha = 1$ e $\alpha^* = 1$. Logo, $b(\alpha) = 1$.

(**cláusula (2)**) $b(\neg\neg\alpha) = F \rightarrow b(\alpha) = F$;
$(\neg\neg\alpha)^* = (\alpha^* \cdot x_\alpha + 1) \cdot x_\alpha + 1 = 0 \Rightarrow (\alpha^* \cdot x_\alpha + 1) \cdot x_\alpha = 1 \Rightarrow x_\alpha = 1$ e $\alpha^* \cdot x_\alpha + 1 = 1$.
Se $\alpha^* \cdot x_\alpha + 1 = 1 \Rightarrow \alpha^* \cdot x_\alpha = 0 \Rightarrow x_\alpha = 0$ ou $\alpha^* = 0$.
Pela restrição, temos como condições de valorações que: $x_\alpha = 1$ e $\alpha^* = 0$. Portanto, $b(\alpha) = 0$.

$(ii) \Rightarrow (i)$

1ºcaso: $b(\neg\neg\alpha) = 0, b(\neg\neg\alpha) = 1$
Ambas já foram demonstradas.
■

4.4 As variáveis ocultas e a verofuncionalidade

O conceito de verofuncionalidade é um dos mais importantes da lógica contemporânea. De acordo com Ryan Young em (Young 2012), apesar de ser uma noção essencial para o desenvolvimento e construção da lógica moderna, as pesquisas a respeito da conceitualização de valor de verdade têm recebido pouca atenção por parte dos pesquisadores. Para o autor, a única base sólida a respeito dessa conceitualização foi a definição de Frege dos valores de verdade clássicos, no final do século XIX.

Para Frege a concepção de valor de verdade era um componente natural da linguagem a ser analisada, onde sentenças são interpretadas como um tipo especial de nomes, que se referem (indicam, designam, significam) a um tipo especial de objetos: valores de verdade. Além disso, há, de acordo com Frege, apenas dois tais objetos: o verdadeiro e o falso.

Ainda de acordo com Ryan Young, há uma fundamental limitação dentro da definição fregeana de valor de verdade: ele define o papel que valor de verdade tem dentro de uma estrutura semântica, mas não diz nada a respeito de que tipo de coisa os valores de verdade são.

Łukasiewicz, em 1918, é tido como o autor que propôs considerarmos outros valores de verdades diferentes do verdadeiro e falso. Em 1920, independentemente de Łukasiewicz, Emil Post introduziu o conceito de n-valor de verdade, onde n é qualquer número inteiro positivo.

A questão de se determinar realmente como a lógica multivalente genuína teria sido introduzido na literatura ainda apaixona os lógicos. Em (Carnielli 2012), Walter Carnielli defende que Paul Bernays deveria ser visto como o verdadeiro precursor das lógicas multivalentes, mesmo Vasiliev tendo idealizado tudo isso, uma vez que teria introduzido tais lógicas tal como os geômetras pensaram nas geometrias alternativas.

Assim, embora o conceito de valor de verdade seja amplamente aplicado dentro da lógica, a falta de uma definição a respeito do que é um valor de verdade, ou quais são de fato os valores de verdade, levanta sérias questões a respeito dos fundamentos da lógicas n-valoradas.

Para da Costa, Beziau e Bueno em (da Costa, Béziau & Bueno 1996), p. 281,

> "Undoubtedly, a fundamental problem concerning many-valuedness is to know what it really is. This may seem a triviality; however, despite the fact that many-valued logic is a wide and prolific field of modern logic, it seems that the question of its very nature has not yet been completely elucidated".

Tanto Ryan Young em (Young 2012), quanto João Marcos em (Marcos 2009), assim como muitos outros pesquisadores, apresentam uma definição formal do que são os valores de verdade. Mais do que isso, João Marcos exibe uma caracterização semântica do fenômeno da verofuncionalidade em 10 máximas. Em resumo, uma lógica $\mathcal{L}$ é dita ser verofuncional sobre um conjunto de sentenças $\mathcal{S}$ se:

1. $\mathcal{L}$ pode ser dada em uma semântica multivalorada;
2. Há pelo menos dois tipos de valores de verdade, os ditos *distinguidos* e *não-distinguidos*;
3. $\mathcal{L}$ tem associada uma relação de consequência;
4. $\mathcal{L}$ tem um caráter algébrico, isto é, o conjunto de sentenças $\mathcal{S}$ é construído como uma álgebra livre;
5. A semântica multivalorada de $\mathcal{L}$ é representativa, no sentido que $SEM[\varphi] \supseteq SEM[\varphi^{\epsilon}]$ onde ϵ é um endomorfismo $\epsilon : \mathcal{S} \to \mathcal{S}$;
6. Os conjuntos $\mathcal{V}$, $\mathcal{D}$ e $\mathcal{U}$ são fixos, para toda $\S \in SEM$;
7. O conjunto de valorações é laplaciano, isto é, $SEM[p] = \mathcal{V}$, para toda $p \in ats$;
8. Há um conjunto de operadores sobre $\mathcal{V}$ de mesmo tipo do conjunto de conectivos cct;
9. Para cada conectivo $c \in cct$ e $\S \in SEM$, $c : \mathcal{V}^m \to \mathcal{V}$ é um mapeamento total;
10. $\S(c(\alpha_0, ..., \alpha_{m-1})) = c(\S(\alpha_0), ..., \S(\alpha_{m-1}))$

Conforme apresentamos na seção precedente, todos os sistemas lógicos que foram reduzidos *à la* Suszko eram, na forma n-valorada, verofuncionais. Os respectivos polinômios, para cada operador, para cada sistema exposto em sua versão verofuncional, são dados por:

- Lógica paraconsistente P_3^1.

$$(\neg x)^* = 2x^2 + x + 2$$
$$(\neg\neg x)^* = x^2 + 2x$$
$$(x \to y)^* = 2x^2 2y^2 + x^2 + 2$$

- Lógica paraconsistente P_4^1.

$$(\neg x)^* = 2x^3 + 3x^2 + 3$$
$$(\neg\neg x)^* = x^2 + 2x$$
$$(\neg\neg\neg x)^* = x^2 + 2x + 3$$
$$(x \to y)^* = 3x^3 y^3 + 3x^3 + 3$$

- Lógica Belnap.

$$(\neg x)^* = 2x^2$$
$$(\neg\neg x)^* = x$$
$$(x \wedge y)^* = x^2y^2 + 3x^2y + 3xy^2$$
$$(x \vee y)^* = x^2y^2 + 3x^2y + 3xy^2 + x + y$$

- LFI1.

$$(x \wedge y)^* = 2x^2y^2 + 2x^2y + 2xy^2 + xy$$
$$(x \vee y)^* = x^2y^2 + x^2y + xy^2 + 2xy + x + y$$
$$(x \to y)^* = 2x^2y^2 + x^2 + y^2 + y + 2$$
$$(\neg x)^* = 2x + 2$$
$$(\bullet x)^* = x^2 + x$$

As lógicas multivalentes, as quais rejeitam o princípio clássico da bivalência, surgiram em decorrência de duas motivações principais: o interesse matemático em um sistema alternativo ao clássico bivalente e, de modo mais filosófico, a insatisfação com a imposição clássica da dicotomia entre o verdadeiro e o falso.

A utilização de sistemas finitários multivalentes são importantes pois envolve questões concernentes aos seguintes fatos:
(i) A questão de se o princípio de bivalência implicaria o determinismo, e portanto, a não-existência do livre arbítrio, conforme apontado por Łukasiewicz (problema dos futuros contingentes);

(ii) Representabilidade de predicados matemáticos que não estão completamente definidos, conforme propôs Kleene com a inserção de um terceiro valor no seu sistema lógico a fim de representar o elemento *matematicamente indecidível*;

(iii) Possibilidade de se trabalhar com sentenças paradoxais, tal como apresentado no sistema trivalente de Bochvar, em que o terceiro elemento representa o *sem sentido*, o *paradoxal*.

(iv) Solubilidade de alguns problemas levantados pela mecância quântica, no sentido apresentado por Reichenbach em sua lógica trivalente, dentre outros.

No entanto, as traduções polinomiais dos sistemas reduzidos P_3^1, P_4^1, Belnap e LFI1, são constituídas por dois conjuntos distintos de variáveis: as proposicionais e as ocultas. Ocorre que, ao serem reduzidos, esses sistemas perdem a verofuncionalidade e a utilização das variáveis ocultas para representar tal fato se faz necessária.

Verofuncionalidade é uma propriedade desejável para os sistemas semânticos, mas não há razão alguma para temer a sua ausência. Há muitas vantagens em se trabalhar com semânticas bivalentes, dentre elas destacamos:

- Uniformidade em sua estrutura, na qual uma infinidade de diferentes lógicas não-clássicas podem ser especificadas e comparadas umas com as outras;
- Estabelicimento da decidibilidade para uma grande gama de lógicas não-clássicas;
- Analiticidade;
- Facilidade na demonstração de teoremas, dentre outros.

Diante desse contexto, é importante salientarmos que os polinômios a serem trabalhados em cada sistema apresentado (n-valente ou bi-valente *à la* Suszko) serão de natureza completamente diferentes. Logo, representações distintas de um mesmo sistema lógico implica em polinômios distintos, com características específicas.

Capítulo 5

A Lógica de Primeira Ordem em uma versão polinômica

> "The art of doing mathematics is finding that special case that contains all the germs of generality"
> (David Hilbert.)

Nos capítulos anteriores mostramos que o método de provas por anéis de polinômios pode ser aplicado a distintos sistemas lógicos, modulando as características específicas de cada um dos sistemas que foram traduzidos. Neste capítulo, desenvolvemos a Lógica de Primeira Ordem (LPO) em uma versão polinômica, por meio da definição de um novo domínio algébrico apto para operar com somas e produtos infinitos.

Obtemos como resultado mais importante do capítulo o teorema da correção e completude em sua versão polinômica através dos seguintes passos:

1. Definimos uma versão da LPO em suas ambas vertentes, sintática e semântica, supondo que sua noção de consequência sintática seja caracterizada pela noção de consequência semântica, como é usual (ou seja, estamos escolhendo uma versão da LPO correta e completa na formulação usual);

2. Definimos um domínio de séries formais generalizadas por produtos que generaliza, ao mesmo tempo, a noção de polinômios finitos e infinitos, denominado **SGP**;

3. Mostramos que **SGP** tem certas propriedades que permitem computar com tais polinômios e definir uma noção de solubilidade;

4. Traduzimos as fórmulas da LPO nos elementos de **SGP** e mostramos que a noção de satisfatibilidade lógica pode ser reduzida à prova finitária, porém com elementos infinitos, de solubilidade algébrica;

5. Como partimos de uma versão correta e completa de LPO, obtemos como consequência que a noção de derivabilidade lógica é igualmente caracterizada pela solubilidade algébrica em **SGP**

5.1 A Lógica de Primeira Ordem (LPO)

A estrutura sintática e semântica da LPO escolhida para ser utilizada neste capítulo é a mesma de Raymond M. Smullyan em "*First Order Logic*", 1995, (Smullyan 1995).

5.1.1 Sintaxe da LPO

A linguagem da lógica de primeira ordem consiste em:

- Símbolos da lógica proposicional, exceto as variáveis proposicionais, sendo $C = (\neg, \wedge, \vee, \rightarrow)$ o conjunto de operadores proposicionais;
- Quantificadores lógicos: Universal ($\forall$) e Existencial ($\exists$);
- Uma lista enumerável de símbolos, chamados variáveis individuais;
- Uma lista enumerável de símbolos (distintos dos anteriores), chamados *parâmetros individuais*;
- Para cada inteiro positivo n, uma lista enumerável de símbolos ditos predicados n-ários, ou predicados de grau n.

É importante salientar que o termo "variável" será aqui entendido como *variável individual* e tais variáveis não devem ser confundidas com as variáveis proposicionais. Usaremos as letras minúsculas "x", "y", "z", com ou sem índices, para denotar variáveis individuais quaisquer. Já as letras "a", "b", "c", com ou sem índices, representarão os parâmetros individuais, ou simplesmente, parâmetros.

Os parâmetros nada mais são do que símbolos arbitrários, mas fixos, da linguagem utilizados com o objetivo de denotar um indivíduo que atende a uma determinada propriedade ou situação. Um exemplo da utilização de parâmetros está na representação dos números ditos racionais, isto é, um número é racional se pode ser escrito na forma $\frac{p}{q}$, com $q \neq 0$ e p, q sem fatores comuns. Neste caso, as letras p e q denotam elementos arbitrários quaisquer que satisfazem as condições citadas.

As letras maiúsculas "P", "Q", "R", com ou sem subscritos, serão utilizadas para denotar os predicados n-ários.

Usaremos o termo *símbolos individuais* para representar, coletivamente, as variáveis individuais e os parâmetros.

(i) Definição de fórmulas na LPO.

Definimos como uma *fórmula atômica* uma (n + 1)-upla $Pc_1, ..., c_n$ em que P é um predicado qualquer de grau n e $c_1, ..., c_n$ são símbolos individuais quaisquer (variáveis ou parâmetros).

A partir do conceito de fórmulas atômicas, definimos que:

1. Toda fórmula atômica é uma fórmula da LPO;
2. Se A e B são fórmulas, então $\neg A$, $A \wedge B$, $A \vee B$ e $A \rightarrow B$ são fórmulas da LPO;

3. Se A é uma fórmula e x uma variável, então $(\forall x)A$ e $(\exists x)A$ são fórmulas da LPO.

Definimos por *fórmulas puras* as fórmulas apresentadas sem parâmetros.

(ii) Substituição

Para qualquer fórmula A, variável x e parâmetro a, definimos A_a^x do seguinte modo:

- Se A é atômica, então A_a^x é o resultado da substituição de todo ocorrência de x em A por a.
- $[A \wedge B]_a^x = A_a^x \wedge B_a^x$;
  $[A \vee B]_a^x = A_a^x \vee B_a^x$;
  $[A \rightarrow B]_a^x = A_a^x \rightarrow B_a^x$;
  $[\neg A]_a^x = \neg[A_a^x]$.
- $[(\forall x)A]_a^x = (\forall x)A$;
  $[(\exists x)A]_a^x = (\exists x)A$.

Mas, para uma variável y, distinta de x, temos:
$[(\forall x)A]_a^y = (\forall x)[A_a^y]$;
$[(\exists x)A]_a^y = (\exists x)[A_a^y]$.

Denotamos por *variável quantificada* a variável que acompanha diretamente o quantificador, isto é, quando é uma variável do tipo $(\forall x)$ ou $(\exists x)$. Em um fórmula A, entendemos por *escopo de uma variável quantificada* a menor fórmula que segue à ocorrência dessa variável.

Assim, definimos uma ocorrência de uma variável x em uma fórmula A como *ligada* se ela está dentro do escopo de alguma ocorrência de $(\forall x)$ ou $(\exists x)$, ou se a própria variável é precedida imediatamente por $\forall$ ou $\exists$. Uma ocorrência de x em uma fórmula A é dita *livre* se não é ligada.

Observemos, também, que é possível definir o que significa dizer que x tem uma ocorrência livre em A, sem precisar conceitualizar a noção de ocorrência. Usando nossa operação de substituição, podemos dizer que x tem uma ocorrência livre em A se, para algum parâmetro a (ou, equivalentemente, para qualquer parâmetro a), A_a^x é distinto de A.

5.1.2 Valorações e modelos de primeira ordem.

Seja U um conjunto qualquer não-vazio denominado *conjunto universo* ou *domínio*. Por uma U-fórmula entendemos uma (n+1)-upla ordenada $P\xi_1, ..., \xi_n$, em que P é um predicado n-ário e cada ξ_i é uma variável proposicional ou um elemento de U. (Note que não é permitido que ξ_i seja um parâmetro.)

Definidas as U-fórmulas atômicas, podemos definir o conjunto de todas as U-fórmulas pelas regras de formação apresentadas no item (i).

Para qualquer elemento $k \in U$, definimos a fórmula F_k^x exatamente do mesmo modo como foi definido F_a^x, em que a é um parâmetro.

Designaremos por E^U o conjunto de todas as U-fórmulas fechadas (ou sentenças), isto é, para qualquer fórmula A, variável x e parâmetro a, $A_a^x = A$. Uma *valoração de primeira ordem* v de E^U, é definida como uma função $v : E^U \rightarrow \{\mathbf{0}, \mathbf{1}\}$ tal que:

1. v é uma valoração booleana de E^U, isto é, para quaisquer X e Y em E^U temos:
   $v(X \wedge Y) = 1$ sse $v(X) = 1$ e $v(Y) = 1$;
   $v(X \vee Y) = 1$ sse $v(X) = 1$ ou $v(Y) = 1$;
   $v(X \to Y) = 1$ sse $v(X) = 0$ ou $v(Y) = 1$;
   $v(\neg X) = 1$ sse $v(X) = 0$.

2. $v((\forall x)A) = 1$ sse para todo $k \in U$, $v(A^x_k) = 1$;
   $v((\exists x)A) = 1$ sse para pelo menos um $k \in U$, $v(A^x_k) = 1$.

Uma valoração atômica de E^U é uma atribuição de valores de verdade a todos os elementos atômicos de E^U.

Seja E o conjunto de todas as fórmulas puras (sem parâmetros) da LPO. Por uma *interpretação* I de E em um universo U, entende-se como uma função que atribui a cada predicado n-ário P, uma relação n-ária P^* de elementos de U.

Uma U-sentença atômica $P\xi_1, ..., \xi_n$ é verdadeira sob I se a n-upla $\xi_1, ..., \xi_n$ estiver na relação P^*. Desse modo, a interpretação I induz a uma única valoração atômica v_0.

Do mesmo modo, se começarmos com uma valoração atômica v_0 em um universo U, podemos associar a essa valoração a interpretação que define cada P^* como o conjunto de todas as n-uplas $\xi_1, ..., \xi_n$ tais que $P\xi_1, ..., \xi_n$ é verdadeira sob v_0. Assim, temos que essa interpretação I é a única que induz de volta v_0.

Portanto, não há uma diferença essencial entre os pontos de vista das interpretações e das valorações atômicas, de modo que usaremos a noção que for mais conveniente em cada circunstância.

(i) Validade e satisfatibilidade.

Uma fórmula pura A é dita *válida* se A é verdadeira para qualquer interpretação (em qualquer universo). Equivalentemente, A é válida se, para qualquer universo U, A é verdadeira sob qualquer valoração de primeira ordem de E^U.

Uma fórmula A é *satisfatível* (em primeira ordem) se é verdadeira em pelo menos uma interpretação e um universo U - equivalentemente, se, para ao menos um universo U, existe pelo menos uma valoração de primeira ordem na qual A é verdadeira.

Em se tratando de um universo específico U, uma fórmula é *válida* em U se é verdadeira em todas as interpretações em U, e é dita ser *satisfatível* em U se é verdadeira em pelo menos uma interpretação em U. Em resumo, uma fórmula A é válida sse A é válida em qualquer universo; A é satisfatível sse é satisfatível em pelo menos um universo.

Até o momento nossas explicações centraram-se em fórmulas puras. Vejamos como são definidos os conceitos de validade e satisfatibilidade em *sentenças com parâmetros*.

Seja A uma sentença contendo exatamente os parâmetros $a_1, ..., a_n$, isto é, da forma $A(a_1, ..., a_n)$. Para qualquer universo U e quaisquer elementos $k_1, ..., k_n$ de U, entenderemos por $A(k_1, ..., k_n)$ o resultado da substituição simultânea de a_1 por k_1, a_2 por k_2, ..., a_n por k_n em $A(a_1, ..., a_n)$. Dada uma interpretação I dos predicados de $A(a_1, ..., a_n)$ no universo U, diremos que $A(a_1, ..., a_n)$ é *satisfatível* sob I, se existir pelo menos uma n-upla $\langle k_1, ..., k_n \rangle$ de U tal que $A(k_1, ..., k_n)$ é verdadeira sob I.

E, $A(a_1, ..., a_n)$ será dita *válida* sob I se, para quaisquer $k_1, ..., k_n$ de U, $A(k_1, ..., k_n)$ for verdadeira sob I.

Do mesmo modo, diremos que uma fórmula A é válida (satisfatível) em U se A for válida (satisfatível) sob todas as interpretações (pelo menos uma interpretação) em U; $A(a_1, ..., a_n)$ é válida (satisfatível) se $A(a_1, ..., a_n)$ for válida (satisfatível) em todos (pelo menos um) universo.

5.2 Séries Formais

A noção de anel de polinômios foi sucintamente exposta no capítulo 1, seção 1.3. Como a partir de agora precisaremos dessas conceitualizações, a exporemos novamente e com mais detalhes de modo que o leitor não precise retornar, a todo momento, ao capítulo 1.

1. Anéis polinomiais.

Faremos nossa análise em polinômios desenvolvidos sobre uma única indeterminada. No entanto, todas e definições e teoremas podem ser generalizados para polinômios com várias indeterminadas.

Seja A um anel (em casos particulares, um corpo). O conjunto

$$A[x] = \left\{p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n, a_i \in A, n \in \mathbb{N}\right\}$$

é denominado *anel de polinômios* sobre A.

As operações de adição e multiplicação entre os elementos de um anel polinomial são definidas do seguinte modo:

(i) Adição entre polinômios

Definição 5.2.1. Seja A um anel comutativo e $f(x)$ e $g(x)$ dois polinômios em $A[X]$, isto é:

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$$

e

$$g(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m$$

define-se

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + ... + (a_p + b_p)x^p$$

onde p é o máximo de m e n, e $a_i = 0$ se $i > n$ e $b_i = 0$ se $i > m$.

(ii) Multiplicação entre polinômios

Definição 5.2.2. Dados dois polinômios em $A[X]$,

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$$

e

$$g(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m$$

define-se

$$f(x).g(x) = \sum_{k=0}^{m+n} c_k x^k = c_0 + c_1 x + c_2 x^2 ... + c_{n+m} x^{n+m}$$

sendo

$$c_k = \sum_{i+j=k} a_i b_j = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + ... + a_k b_0$$

para cada k, $0 \leq k \leq m+n$

Segue-se imediatamente das definições de adição e multiplicação, que $A[x]$ é um anel comutativo.

Teorema 5.2.3. *Seja A um anel comutativo com unidade. Então o conjunto dos polinômios com coeficientes no anel A, em uma indeterminada, é um anel. Isto é, $\langle A, +, . \rangle$ é um anel com unidade.*

Demonstração: Vide (Zariski, Samuel & Cohen 1958), Cap. I, seção 16, p. 25. ∎

Observação 5.2.4. Em polinômios finitos, tais como definimos até o momento, a definição da operação de multiplicação está fundamentada em somas e produtos finitos. Em notação formal, temos

$$\sum_{k=0}^{m+n} \left(\sum_{i+j=k} (a_i b_j) \right) .x^k$$

Veremos que tal não ocorrerá em séries formais generalizadas.

Precisamos, portanto, definir o conceito de séries formais e, consequentemente, o de séries formais generalizadas.

2. Séries Formais.

Leonhard Paul Euler foi um dos maiores mestres no estudo e desenvolvimento das mais diversas áreas da matemática, sendo esses trabalhos reconhecidos pelos matemáticos contemporâneos. Nas palavras de Veeravalli S. Varadarajan, (Varadarajan 2007), p. 515,

> Leonhard Euler is one of the greatest and most astounding icons in the history of science. His work, dating back to the early eighteenth century, is still with us, very much alive and generating intense interest. Like Shakespeare and Mozart, he has remained fresh and captivating because of his personality as well as his ideas and achievements in mathematics.

O nome de Euler está associado a um grande número de temas. Dentre eles, nos ocuparemos das séries formais. Talvez apenas Jacobi e Ramanujam possam ser colocados em um mesmo nível de conhecimento ao de Euler em relação às séries formais.

Apesar de ser um assunto estudado por muitos matemáticos anteriores a ele, tais como Arquimedes, Leibniz e Pietro Mengoli (dentre outros), as séries consideradas para a análise eram formadas apenas por termos positivos. Além disso, os conceitos estudados sobre convergência e divergência eram tratados apenas informalmente.

No século XVII, Pietro Mengoli expôs o problema de se encontrar a soma exata do inverso dos quadrados dos inteiros positivos, isto é:

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + ...$$

Este problema, que mais tarde ficou conhecido como o *Problema de Basiléia*[1] gerou um intenso interesse nos matemáticos da época, principalmente entre os irmãos Jakob e Johann Bernoulli. Euler não apenas resolveu esse problema como também o generalizou.

A prova formulada por Euler parte da série de Taylor para a função seno, ou seja:

$$sen(x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!}.x^{2n+1}$$

para todo x.

E após uma série de cálculos, chega-se ao seguinte resultado:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Uma extensão natural dos anéis de polinômios A[X] sobre A, que vimos no item (1), é definida pelo anel A[[X]] das séries formais, em uma variável, sobre A. Assim, temos:

Definição 5.2.5. Uma **série formal** é uma expressão algébrica definida como

$$A[[X]] = \{a_0 + a_1x + a_2x^2 + ... + a_nx^n + ...\} = \sum_{k=0}^{\infty} a_kx^k,$$

com $a_i \in A, i \in \mathbb{N}$

Os coeficientes a_i podem ser escolhidos a partir de qualquer anel comutativo.

As operações de adição e multiplicação nas séries formais são definidas por:

Definição 5.2.6. (Adição de séries formais) Consideremos duas séries formais em A[[X]], isto é,

$$f(x) = \sum_{k=0}^{\infty} a_kx^k \text{ e } g(x) = \sum_{k=0}^{\infty} b_kx^k,$$

define-se

$$f(x) + g(x) = \sum_{k=0}^{\infty} a_kx^k + \sum_{k=0}^{\infty} b_kx^k = \sum_{k=0}^{\infty}(a_k + b_k)x^k.$$

Definição 5.2.7. (Multiplicação de séries formais) Consideremos duas séries formais em A[[X]], isto é,

$$f(x) = \sum_{k=0}^{\infty} a_kx^k \text{ e } g(x) = \sum_{k=0}^{\infty} b_kx^k,$$

define-se

$$f(x).g(x) = \sum_{k=0}^{\infty} a_kx^k. \sum_{k=0}^{\infty} b_kx^k = \sum_{k=0}^{\infty}(c_k)x^k,$$

onde $c_k = \sum_{j=0}^{k} a_j.b_{k-j}$

[1]Basel, é a cidade da Suíça onde residiam Euler e os irmãos Bernoulli.

5.3 Séries generalizadas por produtos.

Por um período de dez anos, Euler preocupou-se com a expansão de séries formais da função seno. O tema expandiu-se consideravelmente no domínio dos números reais e complexos.

No entanto, para séries abstratas (no sentido de séries formais com produtos e somas infinitas arbitrárias) não há um tratamento algébrico natural, isto é, um domínio no qual possamos operar com produtos e somas infinitas.

Definimos, dessa forma, um domínio que governa o espaço das séries formais generalizadas.

Definição 5.3.1. Um domínio $\mathfrak{D} = \langle \mathbb{P}, +, . \rangle$ tal que:

1. $\mathbb{P}$ é a classe dos produtos finitos ou infinitos do tipo

$$P = \prod_{k=0}^{\infty} a_1 x_{1k}$$

com $a_1 \in \mathbb{Z}_2$ e x_{1k} variáveis (consideramos o caso finito como aquele onde as variáveis são iguais a 1, a menos de um número finito delas, e onde o produto da constante 1 infinitas vezes é igual a 1).

2. $\prod_{k=0}^{\infty} a_1 x_{1k} = 1$ sse $(x_{1k} = 1)$ para todo x_{1k} e $(a_1 = 1)$;

3. $\prod_{k=0}^{\infty} a_1 x_{1k} = 0$ sse $(x_{1k} = 0)$ para algum x_{1k};

4. O produto é fechado por somas finitas, de modo que:

$$\left(\prod_{k=0}^{\infty} a_1 x_{1k} + ... + \prod_{k=0}^{\infty} a_n x_{nk}\right) . \left(\prod_{k=0}^{\infty} b_1 y_{1k} + ... + \prod_{k=0}^{\infty} b_m y_{mk}\right) =$$

$$= \prod_{k=0}^{\infty} (a_1 . b_1) x_{1k} y_{1k} + ... + \prod_{k=0}^{\infty} (a_1 . b_m) x_{1k} y_{mk} + ...$$

$$\vdots$$

$$\prod_{k=0}^{\infty} (a_n . b_1) x_{nk} y_{1k} + ... + \prod_{k=0}^{\infty} (a_n . b_m) x_{nk} y_{mk} + ...$$

5. $\prod_{k=0}^{\infty} (\prod_{i=0}^{\infty} (x_{1k}, y_{1i})) = \prod_{i=0}^{\infty} (\prod_{k=0}^{\infty} (x_{1k}, y_{1i}))$;

6. $(\prod_{k=0}^{\infty} a_1 x_{1k}) . (\prod_{k=0}^{\infty} b_1 y_{1k} . \prod_{k=0}^{\infty} c_1 z_{1k}) = (\prod_{k=0}^{\infty} a_1 x_{1k} . \prod_{k=0}^{\infty} b_1 y_{1k}) . \prod_{k=0}^{\infty} c_1 z_{1k}$;

7. $(\prod_{k=0}^{\infty} a_1 x_{1k}) + (\prod_{k=0}^{\infty} a_1 x_{1k}) = 0$;

8. $(\prod_{k=0}^{\infty} a_1 x_{1k}) .0 = 0 . (\prod_{k=0}^{\infty} a_1 x_{1k}) = 0$;
$(\prod_{k=0}^{\infty} a_1 x_{1k}) + 0 = 0 + (\prod_{k=0}^{\infty} a_1 x_{1k}) = (\prod_{k=0}^{\infty} a_1 x_{1k})$;
$(\prod_{k=0}^{\infty} a_1 x_{1k}) .1 = 1 . (\prod_{k=0}^{\infty} a_1 x_{1k}) = (\prod_{k=0}^{\infty} a_1 x_{1k})$;

é denominado domínio de *séries fomais generalizadas por produtos*, ou sucintamente, **SGP**.

Como estamos admitindo que apenas nos interessa os produtos não-nulos, assumiremos que $(a_1 = 1)$, a menos de menção explícita no texto.

Teorema 5.3.2. *Em um domínio $\mathfrak{D} = \langle \mathbb{P}, +, . \rangle$ de séries generalizadas por produtos (**SGP**), são válidas as seguintes propriedades:*

$(P_1)\,(\prod_{k=0}^{\infty} a_1 x_{1k}) \,.\, (\prod_{k=0}^{\infty} b_1 y_{1k}) = \prod_{k=0}^{\infty} (a_1.b_1) x_{1k}.y_{1k}$;

$(P_2)\,(\prod_{k=0}^{\infty} a_1 x_{1k}) \,.\, (\prod_{k=0}^{\infty} b_1 y_{1k} + \prod_{k=0}^{\infty} c_1 z_{1i}) =$

$(\prod_{k=0}^{\infty} a_1 x_{1k}. \prod_{k=0}^{\infty} b_1 y_{1k}) + (\prod_{k=0}^{\infty} a_1 x_{1k}. \prod_{k=0}^{\infty} c_1 z_{1i})$;

$(P_3)\,(\prod_{k=0}^{\infty} a_1 x_{1k}) \,.\, (\prod_{k=0}^{\infty} a_1 x_{1k}) = (\prod_{k=0}^{\infty} a_1 x_{1k})$.

Demonstração: (a) $(P_1)\,(\prod_{k=0}^{\infty} a_1 x_{1k}) \,.\, (\prod_{k=0}^{\infty} b_1 y_{1k}) = \prod_{k=0}^{\infty} (a_1.b_1) x_{1k}.y_{1k}$.

A prova é uma consequência direta da definição, isto é, por definição temos:

$$\left(\prod_{k=0}^{\infty} a_1 x_{1k} + ... + \prod_{k=0}^{\infty} a_n x_{nk}\right) . \left(\prod_{k=0}^{\infty} b_1 y_{1k} + ... + \prod_{k=0}^{\infty} b_m y_{mk}\right) =$$

$$= \prod_{k=0}^{\infty} (a_1.b_1) x_{1k} y_{1k} + ... + \prod_{k=0}^{\infty} (a_1.b_m) x_{1k} y_{mk} + ...$$

$$\vdots$$

$$\prod_{k=0}^{\infty} (a_n.b_1) x_{nk} y_{1k} + ... + \prod_{k=0}^{\infty} (a_n.b_m) x_{nk} y_{mk} + ...$$

Suponhamos que, para todo $n \neq 1$ e $m \neq 1$, $\prod_{k=0}^{\infty} a_n x_{ni} = 0$ e $\prod_{k=0}^{\infty} b_m y_{mi} = 0$, então:

$$\left(\prod_{k=0}^{\infty} a_1 x_{1k}\right) . \left(\prod_{k=0}^{\infty} b_1 y_{1k}\right) =_{def} \prod_{k=0}^{\infty} (a_1.b_1) x_{1k}.y_{1k}$$

(b) $(P_2)\,(\prod_{k=0}^{\infty} a_1 x_{1k}) \,.\, (\prod_{k=0}^{\infty} b_1 y_{1k} + \prod_{k=0}^{\infty} c_1 z_{1i}) =$
$(\prod_{k=0}^{\infty} a_1 x_{1k}. \prod_{k=0}^{\infty} b_1 y_{1k}) + (\prod_{k=0}^{\infty} a_1 x_{1k}. \prod_{k=0}^{\infty} c_1 z_{1i})$;

$$\left(\prod_{k=0}^{\infty} a_1 x_{1k}\right) . \left(\prod_{k=0}^{\infty} b_1 y_{1k} + \prod_{k=0}^{\infty} c_1 z_{1i}\right) =_{def} \prod_{k=0}^{\infty} (a_1.b_1) x_{1k} y_{1k} + \prod_{k=0}^{\infty} (a_1.c_1) x_{1k} z_{1i}$$

$$=_{P_1} \left(\prod_{k=0}^{\infty} a_1 x_{1k}\right) . \left(\prod_{k=0}^{\infty} b_1 y_{1k}\right) + \left(\prod_{k=0}^{\infty} a_1 x_{1k}\right) . \left(\prod_{k=0}^{\infty} c_1 z_{1i}\right)$$

(c) $(P_3)\,(\prod_{k=0}^{\infty} a_1 x_{1k}) \,.\, (\prod_{k=0}^{\infty} a_1 x_{1k}) = (\prod_{k=0}^{\infty} a_1 x_{1k})$

$= (\prod_{k=0}^{\infty} a_1 x_{1k}) \,.\, (\prod_{k=0}^{\infty} a_1 x_{1k}) =_{P_1} \prod_{k=0}^{\infty} (a_1.a_1) x_{1k}.x_{1k} =$ [2] $\prod_{k=0}^{\infty} a_1 x_{1k}$

■

A partir da estrutura das séries generalizadas por produtos, definiremos os anéis polinomiais para a lógica de primeira ordem (LPO).

[2] Lei do Índice, pela qual $x.x = x$, válida em $\mathbb{Z}_2$

5.3.1 O método de anéis de polinômios para a Lógica de Primeira Ordem

Consideramos, no caso geral, o domínio **SGP** com base em um corpo finito F arbitrário. Embora possamos definir séries generalizadas por produtos com coeficientes em um corpo arbitrário, previlegiaremos a definição no anel $\mathbb{Z}_2$. Reservamos para este caso a notação $\mathbb{Z}_2[\mathbf{SGP}[X]]$, onde X denota as variáveis de **SGP**.

Definição 5.3.3. Seja $X = \{x_{p_1}, x_{p_2}, ...\}$ um conjunto de símbolos individuais. O cálculo de anéis de polinômios para a LPO é definido pela função $*$, que traduz fórmulas de LPO em séries generalizadas por produtos com coeficientes no anel $\mathbb{Z}_2$, o qual denotamos por $\mathbb{Z}_2[\mathbf{SGP}[X]]$, isto é:

$$* : For_{LPO} \to \mathbb{Z}_2[\mathbf{SGP}[X]]$$

tal que:

1. $(p)^* = x_p$, $x_p \in X$. Quando não houver risco de confusão omitiremos o índice em x_p, escrevendo apenas x;
2. $(\alpha \wedge \beta)^* = \alpha^*.\beta^*$;
3. $(\alpha \vee \beta)^* = \alpha^*.\beta^* + \alpha^* + \beta^*$;
4. $(\alpha \to \beta)^* = \alpha^*.\beta^* + \alpha^* + 1$;
5. $(\neg\alpha)^* = \alpha^* + 1$;
6. $(\forall x A(x))^* = \prod_{k=0}^{\infty} a_1 x_{1k}$;
   onde x_{1k} são variáveis em X e $a_1 \in \mathbb{Z}_2$.
7. $(\exists x A(x))^* = 1 + \prod_{k=0}^{\infty}(1 + a_1 x_{1k})$.

Definição 5.3.4. Seja F um corpo, X um conjunto de variáveis e $*$ a função tradução de fórmulas da lógica de primeira ordem $\mathcal{L}$ a polinômios em $\mathbb{Z}_2[\mathbf{SGP}[X]]$. Consideremos $\emptyset \neq D \subset F$ como o conjunto de valores distinguido (embora estejamos interessados apenas em LPO).

Uma fórmula α de $\mathcal{L}$ é uma $\mathcal{L}$-CAP-conseqüência do conjunto de fórmulas Γ de $\mathcal{L}$ (o que será denotado por $\Gamma \mid\!\approx_{\mathcal{L}} \alpha$) se, $\gamma^*[X] \in D$ para toda $\gamma \in \Gamma$ implica que $\alpha^*[X] \in D$, para $\gamma^*[X], \alpha^*[X]$. Em poucas palavras, temos que: Γ acarreta α se, e somente se, o fato que a tradução das fórmulas em Γ pertence a D implica que a tradução de α também pertence a D.

Nos casos em que D é um conjunto unitário ($D = \{d\}$) temos que $\mid\!\approx_{\mathcal{L}} \alpha$ se e somente se α^* é redutível, através das regras do CAP para $\mathcal{L}$, ao polinômio constante d. Embora a definição 5.3.4 tenha sido formulada com vistas a uma lógica multivalente de primeira ordem, no presente trabalho focamos o interesse em LPO. Dessa forma, aqui F é o corpo $\mathbb{Z}_2$ e $D = \{1\}$.

Como exemplo mostraremos, via anéis de polinômios, que todos os esquemas de fórmulas abaixo são válidas para a Lógica de Primeira Ordem. Usaremos para a prova as definições pertinentes e o teorema 5.3.2, indicando a justificativa abaixo do símbolo $\approx$.

1. $\forall x A(x) \to \exists x A(x)$.
Demonstração: $(\forall x A(x) \to \exists x A(x))^* \approx (\forall x A(x))^*.(\exists x A(x))^* + (\forall x A(x))^* + 1 \approx$

$\approx (\prod_{k=0}^{\infty} a_1 x_{1k}).(1 + \prod_{k=0}^{\infty}(1 + a_1 x_{1k})) + \prod_{k=0}^{\infty} a_1 x_{1k} + 1$

$\approx_{P_2} \prod_{k=0}^{\infty} a_1 x_{1k} + \prod_{k=0}^{\infty} a_1 x_{1k}. \prod_{k=0}^{\infty}(1 + a_1 x_{1k}) + \prod_{k=0}^{\infty} a_1 x_{1k} + 1$

$\approx_{P_1} \prod_{k=0}^{\infty} a_1 x_{1k} + \prod_{k=0}^{\infty}(a_1 x_{1k}.(1 + a_1 x_{1k})) + \prod_{k=0}^{\infty} a_1 x_{1k} + 1$

$\approx_{dist} \prod_{k=0}^{\infty} a_1 x_{1k} + \prod_{k=0}^{\infty}(a_1 x_{1k} + a_1 x_{1k}.a_1 x_{1k}) + \prod_{k=0}^{\infty} a_1 x_{1k} + 1$

$\approx_{LI}$ [3] $\prod_{k=0}^{\infty} a_1 x_{1k} + \prod_{k=0}^{\infty} 0 + \prod_{k=0}^{\infty} a_1 x_{1k} + 1$

$\approx_{def_3} \prod_{k=0}^{\infty} a_1 x_{1k} + \prod_{k=0}^{\infty} a_1 x_{1k} + 1$

$\approx_{def_7} 0 + 1$

$\approx 1.$ ∎

2. $\forall x \forall y A(x, y) \Leftrightarrow \forall y \forall x A(x, y)$.
Demonstração: $(\Rightarrow)$
$(\forall x \forall y A(x, y) \to \forall y \forall x A(x, y))^* \approx$

$\approx (\forall x \forall y A(x, y))^* (\forall y \forall x A(x, y))^* + (\forall x \forall y A(x, y))^* + 1$

$\approx \prod_{k=0}^{\infty} (\prod_{i=0}^{\infty}(a_1 x_{1k}, b_1 y_{1i})) \cdot \prod_{i=0}^{\infty} (\prod_{k=0}^{\infty}(a_1 x_{1k}, b_1 y_{1i})) +$
$\prod_{k=0}^{\infty} (\prod_{i=0}^{\infty}(a_1 x_{1k}, b_1 y_{1i})) + 1$

$\approx_{def_5} \prod_{i=0}^{\infty} (\prod_{k=0}^{\infty}(a_1 x_{1k}, b_1 y_{1i})) \cdot \prod_{i=0}^{\infty} (\prod_{k=0}^{\infty}(a_1 x_{1k}, b_1 y_{1i})) +$
$\prod_{k=0}^{\infty} (\prod_{i=0}^{\infty}(a_1 x_{1k}, b_1 y_{1i})) + 1$

$\approx_{P_3} \prod_{i=0}^{\infty} (\prod_{k=0}^{\infty}(a_1 x_{1k}, b_1 y_{1i})) + \prod_{k=0}^{\infty} (\prod_{i=0}^{\infty}(a_1 x_{1k}, b_1 y_{1i})) + 1$

$\approx_{def_5} \prod_{k=0}^{\infty} (\prod_{i=0}^{\infty}(a_1 x_{1k}, b_1 y_{1i})) + \prod_{k=0}^{\infty} (\prod_{i=0}^{\infty}(a_1 x_{1k}, b_1 y_{1i})) + 1$

$\approx_{def_7} 0 + 1$

≈ 1

$(\Leftarrow)$
Análogo ao anterior. ∎

[3] Lei do Índice em $\mathbb{Z}_2$, pela qual $x.x = x$ e $x + x = 0$

3. $\forall x\forall y A(x,y) \to \forall x\exists y A(x,y)$.**Demonstração:** $(\forall x\forall y A(x,y) \to \forall x\exists y A(x,y))^* \approx$

$\approx (\forall x\forall y A(x,y))^*.(\forall x\exists y A(x,y))^* + (\forall x\forall y A(x,y))^* + 1 =$

$\approx (\prod_{k=0}^{\infty}(\prod_{i=0}^{\infty}(x_k,y_i))) \,.\, (\prod_{k=0}^{\infty}(1+\prod_{i=0}^{\infty}(1+(x_k,y_i))) +$
$(\prod_{k=0}^{\infty}(\prod_{i=0}^{\infty}(x_k,y_i))) + 1$

$\approx_{P_1} \prod_{k=0}^{\infty}[(\prod_{i=0}^{\infty}(x_k,y_i)) \,.\, (1+\prod_{i=0}^{\infty}(1+(x_k,y_i))] +$
$(\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(x_k,y_i))) + 1$

$\approx_{P_2} \prod_{k=0}^{\infty}[(\prod_{i=0}^{\infty}(x_k,y_i)) + (\prod_{i=0}^{\infty}(x_k,y_i).\prod_{i=0}^{\infty}(1+(x_k,y_i))] +$
$(\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(x_k,y_i))) + 1$

$\approx_{P_1} \prod_{k=0}^{\infty}[(\prod_{i=0}^{\infty}(x_k,y_i)) + \prod_{i=0}^{\infty}((x_k,y_i).(1+(x_k,y_i))] +$
$(\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(x_k,y_i))) + 1$

$\approx_{dist} \prod_{k=0}^{\infty}[(\prod_{i=0}^{\infty}(x_k,y_i)) + \prod_{i=0}^{\infty}((x_k,y_i)+(x_k,y_i).(x_k,y_i))] +$
$(\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(x_k,y_i))) + 1$

$\approx_{LI}$ [4] $\prod_{k=0}^{\infty}[(\prod_{i=0}^{\infty}(x_k,y_i)) + \prod_{i=0}^{\infty}((x_k,y_i)+(x_k,y_i))] +$
$(\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(x_k,y_i))) + 1$

$\approx_{LI} \prod_{k=0}^{\infty}[(\prod_{i=0}^{\infty}(x_k,y_i)) + \prod_{i=0}^{\infty}(0)] + (\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(x_k,y_i))) + 1$

$\approx_{def_3} \prod_{k=0}^{\infty}[(\prod_{i=0}^{\infty}(x_k,y_i)) + 0] + (\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(x_k,y_i))) + 1$

$\approx_{def_8} \prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(x_k,y_i)) + \prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(x_k,y_i)) + 1$

$\approx_{def_7} 0 + 1$

≈ 1 ∎

4. $\forall x\exists y A(x,y) \to \exists y\exists x A(x,y)$.
Demonstração: $(\forall x\exists y A(x,y) \to \exists y\exists x A(x,y))^* \approx$

$\approx (\forall x\exists y A(x,y))^*.(\exists y\exists x A(x,y))^* + (\forall x\exists y A(x,y))^* + 1$

$\approx (\forall x\exists y A(x,y))^*[(\exists y\exists x A(x,y))^* + 1] + 1$

$\approx \prod_{k=0}^{\infty}(1+\prod_{i=0}^{\infty}(1+(x_k,y_i)).[1+\prod_{i=0}^{\infty}(1+(1+\prod_{k=0}^{\infty}(1+(x_k,y_i))))+1] + 1$

$\approx \prod_{k=0}^{\infty}(1+\prod_{i=0}^{\infty}(1+(x_k,y_i)).\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(1+(x_k,y_i)) + 1$

[4] LI: Lei do índice

$\approx_{def_5} \prod_{k=0}^{\infty}(1+\prod_{i=0}^{\infty}(1+(x_k,y_i)).\prod_{k=0}^{\infty}(\prod_{i=0}^{\infty}(1+(x_k,y_i))+1$

$\approx_{P_1} \prod_{k=0}^{\infty}[(1+\prod_{i=0}^{\infty}(1+(x_k,y_i)).(\prod_{i=0}^{\infty}(1+(x_k,y_i))]+1$

$\approx_{P_2} \prod_{k=0}^{\infty}[\prod_{i=0}^{\infty}(1+(x_k,y_i))+\prod_{i=0}^{\infty}(1+(x_k,y_i)).\prod_{i=0}^{\infty}(1+(x_k,y_i))]+1$

$\approx_{P_3} \prod_{k=0}^{\infty}[\prod_{i=0}^{\infty}(1+(x_k,y_i))+\prod_{i=0}^{\infty}(1+(x_k,y_i))]+1$

$\approx_{def_7} \prod_{k=0}^{\infty}[0]+1$

$\approx_{def_3} 0+1$

≈ 1 ∎

5. $\exists y\forall x A(x,y)\rightarrow\exists y\exists x A(x,y)$.
Demonstração: Sejam $\alpha\equiv\exists y\forall x A(x,y)$ e $\beta\equiv\exists y\exists x A(x,y)$. Assim:

$\alpha^*\equiv(\exists y\forall x A(x,y))^*\approx 1+\prod_{i=0}^{\infty}(1+(1+\prod_{k=0}^{\infty}(1+(x_k,y_i))))$

$\alpha^*\approx 1+\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(1+(x_k,y_i)))$

$\beta^*\equiv(\exists y\exists x A(x,y))^*\approx 1+\prod_{i=0}^{\infty}(1+(1+\prod_{k=0}^{\infty}(1+(x_k,y_i))))\approx 1+\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(1+(x_k,y_i)))$

$\beta^*\approx 1+\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(1+(x_k,y_i)))$

$(\alpha^*\rightarrow\beta^*)^*\approx\alpha^*(\beta^*+1)+1$

$(\alpha^*\rightarrow\beta^*)^*\approx(1+\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(1+(x_k,y_i)))).[1+\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(1+(x_k,y_i)))+1]+1$

$\approx(1+\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(1+(x_k,y_i)))).[\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(1+(x_k,y_i)))]+1$

$=_{P_2} \prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(1+(x_k,y_i)))+\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(1+(x_k,y_i)))(\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}+(x_k,y_i))))$
$+1$

$=_{P_3} \prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}(1+(x_k,y_i)))+(\prod_{i=0}^{\infty}(\prod_{k=0}^{\infty}+(x_k,y_i))))+1$

$\approx_{def_7} 0+1$

$=1$ ∎

6. $\forall x\exists y A(x,y)\rightarrow\exists x\exists y A(x,y)$.
Demonstração:

$(\forall x \exists y A \to \exists x \exists y A)^* \approx$

$\approx (\forall x \exists y A(x,y))^*.[(\exists x \exists y A(x,y))^* + 1] + 1 \approx$

$\approx \prod_{k=0}^{\infty}(1 + \prod_{i=0}^{\infty}(1 + (x_k, y_i))).[1 + \prod_{k=0}^{\infty}(1 + (1 + \prod_{i=0}^{\infty}(1 + (x_k, y_i)))) + 1] + 1$

$\approx \prod_{k=0}^{\infty}(1 + \prod_{i=0}^{\infty}(1 + (x_k, y_i))). \prod_{k=0}^{\infty}(\prod_{i=0}^{\infty}(1 + (x_k, y_i)) + 1$

$\approx_{P_1} \prod_{k=0}^{\infty}[(1 + \prod_{i=0}^{\infty}(1 + (x_k, y_i))).(\prod_{i=0}^{\infty}(1 + (x_k, y_i)))] + 1$

$\approx_{P_2} \prod_{k=0}^{\infty}[\prod_{i=0}^{\infty}(1 + (x_k, y_i)) + \prod_{i=0}^{\infty}(1 + (x_k, y_i)). \prod_{i=0}^{\infty}(1 + (x_k, y_i))] + 1$

$\approx_{P_3} \prod_{k=0}^{\infty}[\prod_{i=0}^{\infty}(1 + (x_k, y_i))) + (\prod_{i=0}^{\infty}(1 + (x_k, y_i)))] + 1$

$\approx_{def_7} \prod_{k=0}^{\infty}[0] + 1$

$\approx_{def_3} 0 + 1$

≈ 1 ∎

7. $\forall x A(x) \wedge \forall x B(x) \Leftrightarrow \forall x(A(x) \wedge B(x))$
Demonstração: $(\Rightarrow)$
$(\forall x A(x) \wedge \forall x B(x) \to \forall x(A(x) \wedge B(x)))^* \approx$

$\approx (\prod_{k=0}^{\infty} x_k. \prod_{k=0}^{\infty} y_k). \prod_{k=0}^{\infty}(x_k.y_k) + (\prod_{k=0}^{\infty} x_k. \prod_{k=0}^{\infty} y_k) + 1$

$\approx_{P_1} \prod_{k=0}^{\infty}(x_k.y_k.x_k.y_k) + \prod_{k=0}^{\infty}(x_k.y_k) + 1$

$\approx_{LI} \prod_{k=0}^{\infty}(x_k.y_k) + \prod_{k=0}^{\infty}(x_k.y_k) + 1$

$\approx_{def_7} 0 + 1$

≈ 1
$(\Leftarrow)$
$(\forall x(A(x) \wedge B(x)) \to \forall x A(x) \wedge \forall x B(x))$
Análogo ao anterior. ∎

8. $\forall x(A(x) \to B(x)) \to (\forall x A(x) \to \forall x B(x))$.
Demonstração:
$(\forall x(A(x) \to B(x)) \to (\forall x A(x) \to \forall x B(x)))^* \approx$

$\approx (\forall x(A(x) \to B(x)))^*.[(\forall x A(x) \to \forall x B(x))^* + 1] + 1$

$\approx \prod_{k=0}^{\infty}(x_k.y_k + x_k + 1).[\prod_{k=0}^{\infty} x_k. \prod_{k=0}^{\infty} y_k + \prod_{k=0}^{\infty} x_k + 1 + 1] + 1$

$\approx_{P_1} \prod_{k=0}^{\infty}(x_k.y_k + x_k + 1).[\prod_{k=0}^{\infty} x_k.y_k + \prod_{k=0}^{\infty} x_k] + 1$

$\approx_{P_2} \prod_{k=0}^{\infty}(x_k.y_k + x_k + 1). \prod_{k=0}^{\infty}(x_k.y_k) + \prod_{k=0}^{\infty}(x_k.y_k + x_k + 1). \prod_{k=0}^{\infty}(x_k) + 1$

$\approx_{P_1} \prod_{k=0}^{\infty}(x_k.y_k + x_k.y_k + x_k.y_k) + \prod_{k=0}^{\infty}(x_k.y_k + x_k + x_k) + 1$

$\approx_{LI} \prod_{k=0}^{\infty}(x_k.y_k) + \prod_{k=0}^{\infty}(x_k.y_k) + 1$

$\approx_{def_7} 0 + 1$

≈ 1 ∎

Uma definição importante para a demonstrabilidade do teorema da completude é o de *solução* para uma U-fórmula (α) em sua versão polinômica (α^*).

Definição 5.3.5. Uma tradução α^* de uma U-fórmula α tem *solução* se, e somente se, existe pelo menos uma atribuição de valores de verdade para as variáveis que compõem α^*, de modo que $\alpha^* = 1$.

Assim podemos dizer que uma fórmula U-fórmula α é *satisfatível* se $\alpha^* = 1$ tem solução.

Do mesmo modo, temos que uma U-fórmula α é *válida* se, e somente se, α é universalmente solúvel, isto é, $\alpha^* = 1$ tem solução para qualquer atribuição de valores de verdade para as variáveis de α^*. Isto significa que para qualquer atribuição de valores de verdade, a tradução polinomial tem solubilidade universal, isto é, as regras reduzem α^* à constante 1.

Uma fórmula é dita *inválida* se, e somente se, ela nunca é solúvel.

Exemplo 5.3.6. A fórmula $(p \vee q \to p)$ tem solução, isto é, é satisfatível pois:

$$(p \vee q \to p)^* = 1 \Leftrightarrow (pq + p + q).p + pq + p + q + 1 = 1 \Leftrightarrow$$

$pq + p + pq + pq + p + q = 0 \leftrightarrow pq + q = 0 \Leftrightarrow q = 0$ ou $p = 1$.

Isto significa que para os casos em que $q = 0$ ou $p = 1$, a fórmula $(p \vee q \to p)$ tem solução.

Exemplo 5.3.7. A fórmula $(p \wedge q \to p)$ é válida.

$$(p \wedge q \to p)^* = 1 \Leftrightarrow (pq).p + pq + 1 = 1 \Leftrightarrow pq + pq + 1 = 1 \Leftrightarrow 1 = 1$$

Isto significa que para qualquer atribuição de valores de verdade para as variáveis p e q, a fórmula $(p \wedge q \to p)$ tem solução.

Exemplo 5.3.8. A fórmula $(p \wedge \neg p)$ é inválida. Isto é:

$$(p \wedge \neg p)^* = 1 \Leftrightarrow p(p + 1) = 1 \Leftrightarrow p + p = 1 \Leftrightarrow 0 = 1$$

Isto significa que para qualquer atribuição de valores de verdade para as variáveis p e q, a fórmula $(p \wedge \neg p)$ não tem solução.

Diante disso, se para uma dada fórmula α, $\alpha^* = 1$ tem solução, isso significa que a aplicação do cálculo de anéis de polinômios para a LPO deduz em um número finito de passos, que α^* reduziu-se a 1. Em outras palavras, a noção de demonstração polinômica é finitária, como se deveria esperar.

Assim, provaremos o teorema mais importante deste capítulo: o teorema da correção e completude na sua forma polinômica. Usaremos, sem perda de generalidade, o próprio conjunto de parâmetros como variáveis.

Teorema 5.3.9. *(Teorema da correção e completude) Seja φ uma U-sentença. Então, em um universo U, $v(\varphi) = 1$ se, e somente se, $\varphi^* = 1$ tem solução em $\mathbb{Z}_2[\boldsymbol{SGP}[U]]$.*[5]

Demonstração: Prova por indução na complexidade de φ.

1) Se φ é atômica.
$v(\varphi) = 1$ sse $\varphi^* = x = 1$ tem solução (a saber, $x = 1$).

2) Se φ é do tipo:

- $\varphi \equiv \psi_1 \wedge \psi_2$;

  Se $\varphi \equiv \psi_1 \wedge \psi_2$, então $v(\psi_1 \wedge \psi_2) = 1 \Leftrightarrow v(\psi_1) = 1$ e $v(\psi_2) = 1$. Por hipótese de indução temos que, $(\psi_1)^* = 1$ tem solução e $(\psi_2)^* = 1$ também tem solução. Isso significa que: $(\psi_1)^*.(\psi_2)^* = 1$ tem solução. Portanto, $(\psi_1 \wedge \psi_2)^* = 1$ tem solução.

- $\varphi \equiv \psi_1 \vee \psi_2$;

  Se $\varphi \equiv \psi_1 \vee \psi_2$, então $v(\psi_1 \vee \psi_2) = 1 \Leftrightarrow v(\psi_1) = 1$ ou $v(\psi_2) = 1$. Por hipótese de indução temos que, $(\psi_1)^* = 1$ tem solução ou $(\psi_2)^* = 1$ tem solução. Isso significa que: $(\psi_1)^*.(\psi_2)^* + (\psi_1)^* + (\psi_2)^* = 1$ tem solução. Portanto, $(\psi_1 \vee \psi_2)^* = 1$ tem solução.

- $\varphi \equiv \psi_1 \rightarrow \psi_2$;

  Se $\varphi \equiv \psi_1 \rightarrow \psi_2$, então $v(\psi_1 \rightarrow \psi_2) = 1 \Leftrightarrow v(\psi_1) = 0$ ou $v(\psi_2) = 1$. Por hipótese de indução temos que, $(\psi_1)^* = 0$ tem solução ou $(\psi_2)^* = 1$ tem solução. Isso significa que: $(\psi_1)^*.(\psi_2)^* + (\psi_1)^* + 1 = 1$ tem solução. Portanto, $(\psi_1 \rightarrow \psi_2)^* = 1$ tem solução.

- $\varphi \equiv \neg\psi$.

  Se $\varphi \equiv \neg\psi$ então $v(\neg\psi) = 1 \Leftrightarrow v(\psi) = 0$. Por hipótese de indução, $(\psi)^* = 0$ tem solução. Consequentemente, $\psi + 1 = 1$ te solução. Portanto, $(\neg\psi)^* = 1$ tem solução.

3) Se φ é do tipo $\forall x\psi(x)$.
Se $\varphi \equiv \forall x\psi(x)$, então, $v(\forall x\psi(x)) = 1$ se, e somente se, para todo $k \in U$, $v(\varphi(k)) = 1$.
Temos que:

$$(\forall x\psi(x))^* = \prod_{k\in K} \psi(k)$$

[5] A rigor, deveríamos nos referir à interpretação $(I_0()^* = v)$, como fizemos nos casos anteriores. Preferimos, contudo, nos referir a "existência de soluções", o qual nos parece ser uma linguagem mais expressiva.

Contudo, $\prod_{k\in K}\psi(k)=1$ tem solução se, e somente se, $(\psi(k))^*=1$ tem solução para todo $k\in U$.

Assim, por hipótese de indução, $v(\forall x\psi(x))=1 \Leftrightarrow (\psi(k))^*=1$ tem solução para todo $k\in U$. Logo, em decorrência da definição 2 do domínio **SGP**, concluímos que:

$$(\forall x\psi(x))^* = (\prod_{k\in K}\psi(k))^* = 1$$

tem solução para todo $k\in U$.

4) Se φ é do tipo $\exists x\psi(x)$.

Se $\varphi\equiv\exists x\psi(x)$, então, $v(\exists x\psi(x))=1$ se, e somente se, para algum $k\in U$, $v(\varphi(k))=1$.

Temos que:

$$(\exists x\psi(x))^* = 1+\prod_{k\in K}(1+\psi(k))$$

Contudo, $1+\prod_{k\in K}(1+\psi(k))=1$ tem solução se, e somente se, $\prod_{k\in K}(1+\psi(k))=0 \Leftrightarrow (\psi(k))^*=1$ tem solução para algum $k\in U$.

Assim, por hipótese de indução, $v(\exists x\psi(x))=1 \Leftrightarrow (\psi(k))^*=1$ tem solução para algum $k\in U$. Assim, em decorrência da definição 3 do domínio **SGP**, concluímos que:

$$(\exists x\psi(x))^* = (1+\prod_{k\in K}(1+\psi(k)))^* = 1$$

tem solução para algum $k\in U$. ∎

Tendo em vista que estamos partindo de uma versão correta e completa da LPO em termos usuais, o teorema anterior tem um corolário imediato em vista da caracterização semântica da LPO:

Corolário 5.3.10. *Seja φ uma sentença de LPO. Então φ é um teorema de LPO sse as regras de **SGP** reduzem φ^* a constante* 1*.*

Demonstração: φ é válida se, e somente se, $v(\varphi)=1$, para toda v, se, e somente se, $\varphi^*=1$ tem solução universal em U, ou seja, se, e somente se, $(\varphi)^*$ se reduz a 1 pelas regras de **SGP**. ∎

Na verdade o que tivemos foi o teorema da completude dito forma fraca ("mas sem esforço pode se obter também o teorema geral da completude, chamado forma forte").

Como um corolário imediato do Teorema da Completude para LPO, obtem-se o Teorema da Compacidade para LPO.

Teorema 5.3.11. *Seja Γ um conjunto de sentenças de LPO, e φ uma sentença de LPO. Então, se $\Gamma\vdash\varphi$ há um subconjunto finito $\Gamma_0\subset\Gamma$ tal que $\Gamma_0\vdash\varphi$.*

Sabemos também que o Teorema da Dedução para LPO não vale sem um cuidado específico no que concerne o uso da Regra de Generalização, a saber: se existe uma prova de φ a partir de $\Delta\cup\psi$ na qual nenhuma aplicação da Regra de Generalização envolve uma variável livre de ψ, então:

$$\Delta\vdash\psi\rightarrow\varphi$$

Isso significa que, se em particular,

$\Delta = \{\psi_1, \cdots, \psi_n\}$ é um conjunto finito, então $\Delta \vdash \varphi$ sse $\vdash (\psi_1 \wedge \cdots \wedge \psi_n) \rightarrow \varphi$.

Referimo-nos a este particular resultado como Teorema da Dedução Cuidadoso para LPO. Demonstrações desses resultados encontram-se em qualquer manual de lógica digno desse nome.

Com base no Teorema da Compacidade e no Teorema da Dedução Cuidadoso para LPO pode-se obter uma "forma forte" do Teorema de Completude para o método LPO.

Teorema 5.3.12. *Seja Γ um conjunto de sentenças de LPO, e φ uma sentença de LPO. Então, $\Gamma \vdash \varphi$ se, e somente se, existe um conjunto finito $\Gamma_0 = \psi_1, \cdots, \psi_n$ de sentenças tal que:*

$$((\psi_1 \wedge \cdots \wedge \psi_n) \rightarrow \varphi)^* \approx 1$$

.

Demonstração:

$\Gamma \vdash \varphi$ sse $\Gamma_0 \vdash \varphi$ para um subconjunto finito $\Gamma_0 \subset \Gamma$ pelo Teorema da Compacidade para **LPO**, sse $\vdash (\psi_1 \wedge \cdots \wedge \psi n) \rightarrow \varphi$ pelo Teorema da Dedução Cuidadoso para LPO, sse $((\psi_1 \wedge \cdots \wedge \psi n) \rightarrow \varphi)^* \approx 1$ pelo Teorema da Completude para **SGP**. ∎

Esta tese dedicou-se a investigar o método de anéis de polinômios para os mais diferentes sistemas lógicos, sejam eles caracterizáveis por matrizes finitas, como no caso das lógicas multivalentes finitárias (determinísticas ou não-determinísticas) ou para sistemas não caracterizáveis por matrizes finitas, como as lógicas paraconsistentes. No entanto, estender o método para a LPO (um objetivo almejado desde o início da pesquisa) fundamentaria ainda mais a característica da universalidade do método. Os conceitos introduzidos neste capítulo talvez possam ser simplificados, mas abrem caminho inclusive para conexões entre álgebra universal e propriedades da lógica de primeira ordem, e pode ser amplamente generalizado, bem como todas as propostas levantadas na tese. Algumas destas perspectivas serão expostas com mais detalhes no próximo capítulo.

Capítulo 6

Conclusões e Perspectivas

O título desta tese, *Demonstrações na algibeira: polinômios como um método universal de prova*, evidência claramente o propósito principal deste trabalho, ou seja, a exposição de um Método Universal de provas.

O método é universal no sentido de constituir um procedimento de prova geral, apto para ser utilizado nos mais diferentes sistemas lógicos.

Há outros sentidos da universalidade, que não coincidem com este, mas que estão relacionados. O que é conhecido como "lógica universal" é o campo da lógica que se preocupa em investigar quais seriam as características comuns a todas as estruturas lógicas. Referências relevantes a respeito são as antologias (Béziau 2007) e (Béziau 2012).

A lógica universal não é nenhuma nova lógica, mas uma teoria geral da lógica, considerada como estruturas matemáticas. O nome foi introduzido na década de 1990 por J.-Y Béziau, mas o tema pode remeter a Alfred Tarski e outros lógicos poloneses como Adolf Lindenbaum, que desenvolveram uma teoria geral da lógica no final da década de 1920, com base em operações de consequência e matrizes lógicas.

Assim como não há nenhuma noção universalmente aceita da lógica (ou de sistema lógico), não há uma noção universalmente aceita de prova, ou de prova enquanto vista como álgebra, e nosso estudo complementa a tarefa da lógica universal.

O interessante, também, é que o método de polinômios funciona como uma ferramenta unificadora, já que oferece um único objeto matemático, os polinômios, para comparar vários aspectos de uma mesma lógica, tal como fizemos com algumas lógicas paraconsistentes, como a mbC, em que definimos sua versão polinômica quando exibida em uma semântica diádica e, do mesmo modo, quando exposta em uma semântica não-determinística.

Outro aspecto importante do método, e já evidenciado nos capítulos precedentes, é a sua capacidade de especificar as características inerentes a cada sistema ao qual ele foi aplicado. Ou seja, se estamos trabalhando com sistemas verofuncionais, os polinômios refletem tal característica e se, no entanto, nossos sistemas forem semi-verofuncionais, variáveis ocultas são introduzidas com a função de especificar essa semi-verofuncionalidade.

Em resumo, temos um procedimento de provas de caráter universal, unificador, capaz de descobrir novos sistemas lógicos ou novas propriedades de sistemas lógicos, que pode resgatar uma abordagem com a álgebra que parece ter sido esquecida desde os trabalhos de Bo-

ole e Leibniz, que oferece uma nova ferramente semântica no tratamento de sistemas lógicos semi-verofuncionais, em que o conceito de provar se resume a realizar operações simples entre polinômios, no qual questões inerentes à eficiência computacional emergem, dentre outros.

Diante disto, o rol de perspectivas de trabalhos futuros que esta tese instaura é interessante e desafiador. Dentre eles, destacamos:

1. Avaliação da eficiência do uso dos anéis de polinômios no problema da completude funcional;

2. Exploração do caráter heurístico do método,

3. Análise da possibilidade de ser, os anéis de polinômios, uma nova forma de algebrização da lógica. Além disso, verificar se essa possível algebrização seria compatível, ou não, com a álgebra cilíndrica;

4. Exploração e análise da complexidade computacional do método: seria o método de anéis de polinômios explosivo em espaço, e consequentemente, em tempo também?

5. Pensar em um tratamento a partir de polinômios na direção da obtenção de semânticas diádicas para lógicas separáveis (no contexto da Hipótese 4.2.6). Nesse sentido, não é difícil imaginar um algoritmo que possa partir de polinômios e restrições e chegar em clausulas diádicas, num programa inverso ao de (Caleiro et al. 2005).

6. Um problema que merece ser destacado (o qual, contudo, não faz parte direta da preocupação desta tese) consiste em comparar, cuidadosamente, nossa prova de completude da LPO com as realizadas por Rasiowa e Sikorski em (Rasiowa & Sikorski 1968) e a de Henkin. Isso, no entanto, é um problema a ser tratado no futuro.

Detalharemos, a seguir, cada uma dessas novas perspectivas de trabalho.

6.1 Completude funcional via polinômios

Um conjunto de conectivos proposicionais é dito ser *funcionalmente completo* se todas as fórmulas podem ser representadas usando apenas este conjunto de conetivos. Alguns autores usam a expressão "função n-valorada de Sheffer" para designar um conjunto unário (isto é, uma única função m- ária) que gera todas as funções de verdade em uma dada lógica proposicional de n-valores. Em termos práticos, a questão geral se restringe a conectivos unários e binários, o que também adotamos aqui.

O problema de decidir se uma dada lógica n-valorada tem um conjunto funcionalmente completo de conectivos, e de caracterizar todos os conjuntos funcionalmente completos, é antigo e ainda merece muitas publicações.

Mostraremos que o método de anéis de polinômios pode proporcionar uma nova abordagem para o problema, com perspectivas muito interessantes.

Em (Maksimovic & Janicic 2006), os autores identificam condições suficientes e necessárias para um conectivo proposicional ser funcionalmente completo. Mostraremos que isso também pode ser realizado em termos de polinômios.

Considerando um teorema fundamental (teorema 1.4.1 do capítulo 1, seção 1.4) que mostra que toda função finitária de A $x...x$ A em A, para A finito, pode se representada por polinômios com coeficientes 0, 1, 2, ..., n em um corpo, e que todo polinômio consiste apenas de somas e produtos, obtemos imediatamente o seguinte teorema de caracterização:

Teorema 6.1.1. *Um conjunto de conectivos proposicionais (em particular, uma função de Sheffer) em uma lógica n-valorada é funcionalmente completo se, e somente se, definem as constantes 0, 1, ..., n, a soma e o produto.*

Demonstração: Consequência imediata dos teoremas e definições apresentados acima (ver capítulo capítulo 1, seção 1.4). ∎

Como um exemplo de aplicação desse critério, examinaremos a lógica trivalorada de Charles Pierce. Em três páginas de suas notas inéditas escritas antes de 1910, Charles S. Peirce desenvolveu uma semântica trivalorada para uma lógica trivalorada. Isso aconteceu 10 anos antes da dissertação de Emil Post, a qual é usualmente citada como a obra onde está a origem da lógica trivalorada.

Em suas notas, Pierce usa três símbolos para representar os valores de verdade: V, L e F. Ele associa o V com o valor de verdade "1" e "T", indicando verdade; o F está associado com o valor de verdade "0" e "F", indicando a falsidade; e o L é associado ao valor "$\frac{1}{2}$" e "N", indicando um valor intermediário ou desconhecido.

A lógica trivalorada de Pierce tem duas operações básicas:

1. Operador barra, quando aplicado ao elemento desconhecido retorna desconhecido, e quando aplicado ao valor falso, retorna o valor verdadeiro.

x	V	L	F
$-x$	F	L	V

2. O operador Z, um operador binário que Pierce define como segue:

	V	L	F
V	V	L	F
L	L	L	F
F	F	F	F

Em termos de polinômios, o operador barra (-) corresponde a:

$$f(x) = 2x + 2$$

Por sua vez, o operador Z corresponde ao seguinte polinômio:

$$g(x, y) = x^2y^2 + x^2y + xy^2 + 2xy + x + y$$

interpretando os valores de verdade V, L e F como, respectivamente, 0, 1 e 2.

Podemos facilmente verificar, como um exemplo, que a lógica trivalorada de Pierce não é funcionalmente completa. De fato, os polinômios f e g quando restritos a 0, 2, dão-nos sempre os valores 0, 2, e ainda f(1) = 1 e g(1,1) = 1. Já que 1 + 1 = 2 no corpo $\mathbb{Z}_3$, então não há uma combinação possível de f e g que, quando aplicada ao valor 1, retorne o valor 2. Portanto, a lógica tri-valorada de Pierce não é funcionalmente completa.

Como um outro exemplo, temos o seguinte teorema de Reiner Hähnle:

Teorema 6.1.2. *(Completude funcional de lógicas regulares) Para qualquer n, há uma lógica regular L com n valores de verdade que é funcionalmente completa.*

Tendo em vista o teorema 6.1.1 é totalmente óbvio: para qualquer n, a lógica L com n valores de verdade, que tem os correspondentes operadores para f(x,y) = x.y e g(x, y) = x + y é funcionalmente completa.

6.2 Um procedimento heurístico?

Em "Formal polynomials, heuristics and proofs in logic", (Carnielli 2010), 2010, o método de polinômios é visto como uma ferramenta heurística, por meio da descoberta das chamadas *quarter - logics* (uma generalização das half-logics) e da descoberta de um formalismo apropriado para expressar algumas ideias sobre as conhecidas *leis da forma*.

Há na literatura uma abundância de conectivos não-verofuncionais, tais como a negação parcial($\neg_1$) definida por Jean-Yves Beziau em (Béziau 1999), de modo que:

$$v(\neg_1 P) = 0 \text{ se } v(P) = 1.$$

Embora seja de caráter não-verofuncional, a negação ($\neg_1$) é definida por um processo determinístico limitado, no sentido que $v(\neg_1 P) \in \{0, 1\}$ se $v(P) = 0$, isto é, não há lacunas (buracos) nos valores de verdade.

Quando isso ocorre, toda tabela finito-valorada definida não-determinísticamente, mas de modo limitada, pode ser representada por anéis de polinômios, com variáveis ocultas, com coeficientes em corpos finitos. Assim, a negação $\neg_1 P$ é traduzida por $x.(p + 1)$. No entanto, ao aplicarmos o método de polinômios em $P \to \neg_1 P$ temos que $p.(x.(p + 1)) + p + 1 = p + 1$, mas $p+1$ representa a negação clássica. Na realidade, nosso método demonstra que isso é uma mera consequência da função de composicionalidade. Para maiores detalhes, ver (Carnielli 2009).

Vejamos como ocorre a descoberta das quarter-logicas. Consideremos um conectivo binário definido, semanticamente, em p e q por $x.(p + 1).q$, o qual corresponde a um conectivo não-verofuncional $\rightharpoonup$, cuja condição de valoração é dada por:

$$v(P \rightharpoonup Q) = 0 \text{ se } v(P) = 1 \text{ ou } v(Q) = 0$$

Seja, $K/4$ a quarter-logic definida na assinatura $\{\to, \rightharpoonup\}$. Demonstraremos, via anéis de polinômios, que a negação clássica pode ser definida em termos de $K/4$, recuperando assim o CPC. De fato, podemos definir a negação clássica $\sim$ por:

$$P \to (P \to Q)$$

Em termos polinomiais temos:

$$p.(x.(p+1).q) + p + 1 = p + 1$$

Assim, todo o CPC é recuperado na assinatura $\{\to, \rightharpoonup, \sim\}$.

Para maiores detalhes e explicações sobre o tema, ver (Carnielli 2009). Um estudo mais profundo das potencialidades do método como instrumento heurístico ainda está para ser realizado.

6.3 Anéis de polinômios: um novo olhar sobre a algebrização da lógica?

A concepção de se algebrizar a lógica iniciou-se no século XIX com a tentativa de se conectar duas abordagens independentes na pesquisa em lógica: a noção de equivalência lógica e as noções de asserção e inferência. O programa formalista de David Hilbert, em poucas palavras, estimulou a tendência das pesquisas em lógica a se focarem em torno das noções formais de asserção e inferência lógica.

Tarski, baseado nas ideias de Lindenbaum de ver o conjunto das fórmulas como uma álgebra com operações induzidas por conectivos lógicos, foi quem primeiro descreveu uma conexão entre essas duas abordagens para a lógica, como exposto em seu artigo *Grundzüge des Systemenkalküls*, no qual o autor investiga as bases para a algebrização do cálculo proposicional clássico, por meio do que ele chama de *álgebra da lógica* (ver capítulo 1).

A definição de álgebra, no sentido geral e abstrato, pode ser vista como em (Rasiowa & Sikorski 1968).

Definição 6.3.1. Uma álgebra abstrata, ou simplesmente álgebra, é qualquer par $\left\langle A; \{o_\varphi\}_{\varphi\in\Phi} \right\rangle$, onde A é um conjunto não-vazio (denominado Universo) e, para toda $\varphi \in \Phi$, o_φ é uma operação em A.

Para se algebrizar uma lógica devemos, inicialmente, definir uma álgebra a partir do sistema lógico ao qual pretendemos algebrizar de tal modo que esta álgebra retrate a essência da lógica, ou seja, que esta álgebra expresse as propriedades do sistema lógico em questão. Denominamos por *álgebra das fórmulas* a álgebra desenvolvida a partir da assinatura da lógica, cujo universo é composto pelas fórmulas do sistema lógico e suas operações são definidas a partir dos conectivos da lógica.

Nas últimas décadas, a área de atuação da lógica tem se expandido vertiginosamente em decorrência da sua vasta aplicabilidade em diversas áreas do conhecimento, tal como computação, linguística, etc. A partir do momento que a aplicabilidade da lógica faz com que o sistema do Cálculo Proposicional não seja suficiente para fundamentar estas novas teorias, novos sistemas e consequentemente novas lógicas são desenvolvidas, e portanto, há a necessidade de termos álgebras cada vez mais abstratas para traduzir esses novos sistemas. Podemos citar, como exemplos, as álgebras cilíndricas para a algebrização da LPO, as álgebras de Post para a algebrização das lógicas n-valentes e infinito-valentes de Łukasiewicz, dentre outros.

Ocorre que, para George Boole álgebra e lógica não tinham aspectos completamente distintos. Na realidade, Boole converteu a lógica em um tipo de álgebra simples e intuitiva, onde as principais operações envolvidas nessa álgebra são as de adição e multiplicação. No entanto, em abordagens contemporâneas da lógica, vemos que álgebra e lógica estão radicalmente diferentes e que suas interconexões estão cada vez mais complicadas e não-intuitivas.

Seria, então, o método de anéis de polinômios, cujas operações inerentes a eles resumem-se a adição e multiplicação, uma nova forma de algebrização da lógica? Se sim, qual e como seria o elemento algébrico responsável pela representação das variáveis ocultas ocorridas nos polinômios? Que relações existiriam entre essa possível álgebra e as álgebras cilíndricas? Questões como essas obtém formidáveis perspectivas em futuras pesquisas sobre o tema.

6.4 Eficiência computacional

A complexidade computacional é uma área da ciência da computação que busca determinar por quais motivos certos problemas ditos decidíveis são tão difíceis de serem resolvidos pelos computadores. Sendo assim, a teoria da complexidade computacional estuda a classificação de problemas com base na complexidade dos algoritmos que os resolvam.

Um problema é dito *difícil* se a sua solubilidade requer recursos significativos para qualquer que seja o algoritmo utilizado. A teoria da complexidade computacional formaliza esta ideia por meio da introdução de modelos matemáticos de computação para estudar estes problemas e quantificar os recursos necessários para resolvê-los, tais como tempo e armazenamento.

Para medir a eficiência de um algoritmo frequentemente usamos um tempo teórico que o programa leva para encontrar uma resposta em função dos dados de entrada. Sendo assim, o tempo de execução depende, em geral, das instâncias dos dados de entrada, ou seja, instâncias maiores exigirão mais tempo para resolver. Assim, o tempo necessário para resolver um problema (ou o espaço necessário, ou qualquer outra medida de complexidade) é calculado em função do tamanho da instância. Isso geralmente leva em consideração o tamanho da entrada em bits.

Um algoritmo é denominado polinomial (exponencial) quando sua complexidade é uma função polinomial (exponencial) no tamanho da entrada. Um algoritmo é dito ser eficiente quando sua complexidade é um polinomial no sentido acima.

Seria, o método de anéis de polinômios, explosivo em tamanho, e consequentemente, em espaço? Ou sua complexidade é análoga à complexidade das tabelas verdade?

De fato, uma crítica a respeito do tamanho das fórmulas escritas em uma versão polinômica é pertinente. Mas o mesmo ocorre com as tabelas de verdade à medida que aumentamos as premissas utilizadas no argumento. No entanto, provar em sistemas polinomiais pode ser um procedimento muito mais intuitivo e natural do que por meio da utilização de tabelas de verdade ou pelo método de tablôs, já que tudo se reduz a realizar simples operações de adição e multiplicação.

Como demonstrado em (D'Agostino 1992), tablôs analíticos tais como propostos por Smullyan, não conseguem simular polinomialmente as tabelas- verdade (para a lógica clássica, pelo menos, mas certamente para outras lógicas). Assim os tablôs, sem dispositivos adicionais (como no caso dos chamados KE-tablôs e outros métodos) são inerentemente piores do que tabelas-verdade.

Tal como no caso do sistema KE para a lógica clássica, é esperado que nosso tratamento polinomial tenha um desempenho melhor, em termos de complexidade de prova, do que os tablôs convencionais, e pelo menos comparáveis ao método das tabelas-verdade. De fato, conjecturamos que o Cálculo de Anéis de Polinômios possa simular polinomialmente as tabelas- verdade em todos os casos (determinist́co e não determinísticos). Mas esta conjectura tem de esperar por sua vez.

Bibliografia

Agudelo, J. C. & Carnielli, W. A. (2011). Polynomial ring calculus for modal logics: a new semantics and proof method for modalities, *The Review of Symbolic Logic* **4**: 150–170.

Amo, S., Carnielli, W. A. & Marcos, J. (2002). A logical framework for integrating inconsistent information in multiple databases, *Proceedings of the Second International Symposium on Foundations of Information and Knowledge Systems*, FoIKS '02, Springer-Verlag, London, UK, pp. 67–84.

Arruda, A. I. (1990). *N. A. Vasiliev e a lógica paraconsistente*, Coleção CLE: Centro de Lógica, Epistemologia e História da Ciência, Centro de Lógica, Epistemologia e História de Ciência, UNICAMP.

Avron, A. (2007). Non-deterministic semantics for logics with a consistency operator, *Journal of Approximate Reasoning* **45**: 271–287.

Avron, A. (2008). 5-valued non-deterministic semantics for the basic paraconsistent logic mCi, *Studies in Logic, Grammar and Rhetoric* **14**: 127–136.

Avron, A. & Konikowska, B. (2005). Proof systems for logics based on non-deterministic multiple-valued structure, *Logic Journal of the IGPL* **13**: 365–387.

Avron, A. & Levi, I. (2005). *Non-deterministic multi-valued structures* **15**: 241–261.

Avron, A. & Zamansky, A. (2011). Non-deterministic semantics for logical systems - a survey, *in* F. G. D. Gabbay (ed.), *Handbook of Philosophical Logic*, Kluwer, pp. 227–304.

Béziau, J. Y. (1999). Classical negation can be expressed by one of its halves, *Logic Journal of the Interest Group in Pure and Applied Logics* **7**: 145–151.

Béziau, J. Y. (2007). *Logica universalis: towards a general theory of logic*, Springer.

Béziau, J. Y. (2012). *Universal Logic: an Anthology - Form Paul Hertz to Dov Gabbay*, Springer.

Boole, G. (1951). *The Mathematical Analysis of Logic, Being an Essay Towards a Calculus of Deductive Reasoning*, Cambridge: Macmillan, Barclay, Macmillan.

Boyer, C. B. & Merzbach, U. C. (1991). *A history of mathematics*, Wiley.

Bueno-Soler, J. (2004). *Semânticas algébricas de traduções possíveis*, Master's thesis, IFCH-UNICAMP, Campinas, Brazil.

Bueno-Soler, J. & Carnielli, W. A. (2005). Possible-translations algebraization for paraconsistent logics, *Bulletin of the Section of Logic* **34**: 77–92.

Buss, S. R. (1998). Introduction to proof theory, *Handbook of Proof Theory* **137**: 1–78.

Caleiro, C., Carnielli, W. A., Coniglio, M. E. & Marcos, J. (2005). Two's company: "The Humbug of many logical values", *in* J.-Y. Béziau (ed.), *Logica Universalis*, Birkhauser Verlag, Basel, pp. 169–189.

Caleiro, C. & Marcos, J. (2010). Two many values: An algorithmic outlook on Suszko's thesis, *Multiple-Valued Logic, IEEE International Symposium* pp. 93–97.

Carnielli, W. A. (2000). Possible-translations semantics for paraconsistent logics, *in* D. Batens, C. Mortensen, G. Priest & J. P. Van Bendegem (eds), *Frontiers of Paraconsistent Logic: Proceedings of the I World Congress on Paraconsistency*, Logic and Computation Series, Baldock: Research Studies Press, King's College Publications, pp. 149–163.

Carnielli, W. A. (2001). A polynomial proof system for Lukasiewicz logics, *Second Principia International Symposium*, pp. 6–10.

Carnielli, W. A. (2005a). Polynomial ring calculus for logical inference, *CLE e-Prints* **5**: 1–17.

Carnielli, W. A. (2005b). Polynomial ring calculus for many-valued logics, *Proceedings of the 35th International Symposium on Multiple-Valued Logic*, IEEE Computer Society. Calgary, Canada, pp. 20–25.

Carnielli, W. A. (2007). Polynomizing: Logic inference in polynomial format and the legacy of Boole, *in* L. Magnani & P. Li (eds), *Model-Based Reasoning in Science, Technology, and Medicine*, Vol. 64 of *Studies in Computational Intelligence*, Springer, pp. 349–364.

Carnielli, W. A. (2009). Formal polynomials and the Laws of Form, *Dimensions of Logical Concepts; Béziau, JY, Costa-Leite, A., Eds* .

Carnielli, W. A. (2010). Formal polynomials, heuristics and proofs in logic, *Logical Investigations* **16**: 280–294.

Carnielli, W. A. (2012). Paul Bernays and the eve of non-standard models in logic, *Logica Universalis* **1**: 33–42.

Carnielli, W. A., Coniglio, M. E. & Marcos, J. (2007). Logics of Formal Inconsistency, *Handbook of Philosophical Logic* **14**: 15–107.

Carnielli, W. A. & Lima-Marques, M. (1999). Society semantics and multiple-valued logics, *Advances in Contemporary Logic and Computer Science* **1**: 33–52.

Carnielli, W. A. & Marcos, J. (1999). Limits for paraconsistent calculi, *Notre Dame Journal of Formal Logic* **40**(3): 375–390.

Carnielli, W. A., Marcos, J. & Amo, S. (2000). Formal inconsistency and evolutionary databases, *Logic and Logical Philosophy*, Vol. 8, pp. 115–152.

da Costa, N., Béziau, J. Y. & Bueno, O. (1996). Malinowski and Suszko on many-valued logics: On the reduction of many-valuedness to two-valuedness, *Modern Logic* **6**(1): 272–299.

D'Agostino, M. (1992). Are tableaux an improvement on truth-tables? Cut-free proofs and bivalence, *Journal of Logic, Language, and Information* **1**: 235–252.

Eves, H. (1969). *An introduction to the History of Mathematics*, 3 edn, Holt, Rineharh and Winston.

Fonte, R. A. M. (1983). *N. A. Vasiliev e a lógica não-clássica*, Master's thesis, IFCH-UNICAMP, Campinas, Brazil.

Franci, R. (1988). Antonio de' Mazzinghi: An algebraist of the 14th century, *Historia Mathematica* **15**(3): 240–249.

Givant, S. & Halmos, P. (1974). *An algebraic approach to non-classical logics*, Elsevier: New York.

Givant, S. & Halmos, P. (2009). *Introduction to Boolean Algebras*, Springer.

Halmos, P. (1962). *Algebraic logic*, New York: Chelsea Publishing Co.

Henkin, L. & Tarski, A. (1961). Cylindric algebras, *Lattice Theory, Proceedings of Symposia in Pure Mathematics 2* **34**: 83–113.

Janssen, T. M. V. (2001). Frege, contextuality and compositionality, *Journal of Logic, Language and Information.* **10**(1): 115–136.

Maksimovic, P. & Janicic, P. (2006). Simple characterization of functionally complete one-element sets of propositional connectives, *Mathematical Logic Quarterly* **52**(5): 498–504.

Marcos, J. (2009). What is a non-truth-functional logic?, *Studia Logica* **92**: 215–240.

Martzloff, J. C. (2006). *A History of Chinese Mathematics*, Springer-Verlag.

Quine, W. V. O. (1973). *The Roots of Reference*, Open Court.

Rasiowa, H. & Sikorski, R. (1968). *The Mathematics of Metamathematics*, PWN, Warschau.

Sette, A. M. (1973). On the Propositional Calculus P^1, *Mathematica Japonicae* **18**(13): 173–180.

Sher, G. (2001). Truth, logical structure and compositionality, *Synthese* **126**(1-2): 195–219.

Simon, I. (1981). *Configurações combinatórias*, Instituto de Matemática Pura e Aplicada.

Skolem, T. (1913). Om konstitutionen av den identiske kalkuls grupper, *Proceedings of the 3rd Scandinavian mathematical congress, Kristiania*, pp. 149–163. Tradução em Inglês como On the structure of groups in the identity calculus.

Smullyan, R. M. (1995). *First-Order Logic*, Dover books on advanced mathematics, Dover Publications.

Struik, D. J. (1948). *A Consice History of Mathematics*, Vol. I, Dover Publications: New York.

Tarski, A. (1941). On the calculus of relations, *The Journal of Symbolic Logic* **6**: 73–89.

Varadarajan, V. S. (2007). Euler and his work on infinite series, *Bulletin of the American Mathematical Society* **44**: 515–539.

Whitehead, A. N. (1898). *A Treatise on Universal Algebra*, Cambridge, CUP.

Young, R. (2012). What is a truth value?, *Refereed for the Special Volume of Studia Logica devoted to Truth Values* pp. 1–14.

Zariski, O., Samuel, P. & Cohen, I. S. (1958). *Commutative Algebra II*, Commutative Algebra-Volume I, D. Van Nostrand Company.