SOBRE O MÉTODO DE CÁLCULO COM ANEL DE POLINÔMIOS: ANTECEDENTES HISTÓRICOS E POSSIBILIDADES DE PESQUISA

ON THE POLYNOMIAL RING CALCULUS: HISTORICAL BACKGROUND AND RESEARCH POSSIBILITIES

Fábio Maia Bertato[1]

Resumo: Este artigo aborda os antecedentes históricos e as possibilidades do método de Cálculo com Anéis de Polinômios (**PRC**), por meio do estudo de sua aplicabilidade a diversas lógicas e, em particular, sobre o possível desenvolvimento deste sistema algébrico de prova aplicado à Lógica de Primeira Ordem.

Palavras-chave: Lógica; Anéis de Polinômios; Algebrização; Lógicas Clássicas e Não-Clássicas.

Abstract: In this paper we consider the historical background and the possibilities of the method of the Polynomial Ring Calculus (**PRC**), studying some of its applicability to different logics and, in particular, the possible development of this algebraic system of proof applied to the First Order Logic.

Keywords: Logic; Polynonial Rings; Algebrization; Classical and Non-Classical Logics.

***

1 - Considerações históricas

Durante a Idade Média, por tradição greco-romana, o indivíduo culto era educado no sistema das Sete Artes Liberais. Tal sistema consistia no estudo do *Trivium* e do *Quadrivium*. O *Trivium*, que representava as Humanidades, consistia da Gramática, Retórica e Dialética (Lógica). Os mais avançados estudavam então as Matemáticas: a Aritmética, a Geometria, a Astronomia e a Música, disciplinas que compunham o *Quadrivium*. Os versados nestas podiam então se dedicar às investigações da Filosofia, Teologia, Direito e Medicina, ver [1] [2] e [3]. Nota-se que a Lógica, considerada como criação de Aristóteles, não era classificada como uma disciplina matemática. Todavia, sua influência é evidente nas obras dos matemáticos desde tempos mais remotos. A obra Os *Elementos* de Euclides é um exemplo da marca indelével da Lógica aristotélica aplicada, especialmente quando se compara o método dedutivo euclidiano com o conjunto de textos conhecidos por *Organon*.

[1] Pesquisador (Carreira Pq da Unicamp) do Centro de Lógica, Epistemologia e História da Ciência (CLE - Unicamp). E-mail: *fmbertato@cle.unicamp.br.*

https://doi.org/10.36311/1984-8900.2013.v5n10.4529

A Lógica contemporânea é um ramo da Matemática e da Filosofia. Nas universidades de todo mundo é possível averiguar-se a existência de cursos de Lógica em departamentos de ambas, com intenso intercâmbio. A Lógica, ciência do raciocínio válido, está subjacente a todas as investigações no domínio do puramente racional e converteu-se em disciplina matemática ([4]). Tal conversão tem raízes nos trabalhos de Leibniz, Peacock, De Morgan, Boole, Frege e Gödel,[2] entre outros.

Leibniz é considerado o primeiro a desenvolver uma lógica simbólica. Seu simbolismo, denominado *characteristica universalis*, poderia representar relações lógicas e constituir a base para uma álgebra lógica, o *calculus ratiocinator*, ver [7]. Tais ferramentas permitiriam que quaisquer desacordos entre indivíduos ou nações fossem solucionados por meio de simples cálculos.[3]

Consideramos que os primeiros passos dados por George Peacock (1791 - 1858) e Augustus De Morgan (1806 - 1871) na "libertação" da Álgebra muito influenciaram no desenvolvimento da Lógica Matemática. Peacock distinguiu em sua obra *Treatise on Algebra* (1845) dois tipos de álgebra: a "álgebra aritmética" e a "álgebra simbólica", ver [8]. A primeira era a aritmética universal dos reais não-negativos e os símbolos representavam tais números e as operações com os mesmos. Já na "álgebra simbólica" os símbolos independiam de qualquer particular interpretação. As operações com os símbolos eram derivadas das manipulações com os números ([9]).

De Morgan reconheceu que as leis da Álgebra poderiam ser criadas independentemente de analogias com a Aritmética. Basicamente, De Morgan defendia que um sistema algébrico poderia ser criado a partir de certos símbolos e um conjunto de regras para operá-los, sendo uma interpretação algo *a posteriori* ([9]).[4] Apesar disso, não criou um sistema que obedecesse regras distintas da Aritmética.

---

[2] A bem conhecida importância deste último pode ser resumida com as palavras de Simon Kochen (segundo R. Goldstein): *"Gödel pôs a lógica no mapa matemático. Todo departamento matemático importante agora tem um representante da lógica em sua equipe. Podem ser apenas um ou dois lógicos, mas pelo menos haverá alguém"* ([5]).

[3] *"Quo facto, quando orientur controversiae, non magis disputatione opus erit inter duos philosophos, quam inter duos computistas. Sufficiet enim calamos in manus sumere sedereque ad abacos et sibi mutuo...dicere, calculemus!"* [*"Quando surgissem controvérsias, não seria necessário a disputa entre dois filósofos senão de dois calculistas. Para tanto seria suficiente que tomassem seus lápis em mãos, sentassem juntos a seus ábacos e dissessem um ao outro...: Calculemos!"*] ([6]).

[4] *"We may try this in a small way with three symbols, and one rule of connexion. Given symbols M, N, +, and one sole relation of combination, namely that M + N is the same result (be it of what kind soever) as N + M. Here is a symbolic calculus: how can it be made a significant one? In the following ways, among others. 1. M and N may be* magnitudes*, + the sign of addition of the second to the first. 2. M and N may be* numbers*, and + the sign of multiplying the first by the second. 3. M and N may be* lines*, and + a direction to make a rectangle with the antecedent for a base, and the consequent for an altitude. 4. M and N may be* men*, and + the assertion that the antecedent is the brother of the consequent. 5. M and N may be* nations*, and + the sign of the consequent having fought a battle with the antecedent: and so on"* ([10])

Coube a George Boole (1815 - 1864) a tarefa de explorar tal liberdade algébrica e levar o estudo da Lógica ao domínio da Matemática.[5] Boole publicou suas idéias em um pequeno livro intitulado *The Mathematical Analysis of Logic* (1847) e ampliando-o, publicou em 1854 sua famosa obra *An Investigation of the Laws of Thought*. O objetivo de Boole em sua obra era investigar as leis fundamentais das operações da mente, pelas quais o raciocínio se desenvolve, e dar a essas operações uma linguagem simbólica de um Cálculo, para servir de fundamento da Lógica, ver [12]. A primeira proposição de sua obra é bastante representativa de suas idéias:

> *"Proposition I.*
>
> *All the operations of Language, as an instrument of reasoning, may be conducted by a system of signs composed of the following elements, viz.:*
>
> *1st. Literal symbols, as x, y, &c., representing things as subjects of our conceptions.*
> *2nd. Signs of operation, as +, -, x, standing for those operations of the mind by which the conceptions of things are combined or resolved so as to form new conceptions involving the same elements.*
> *3rd. The sign of identity, =.*
>
> *And these symbols of Logic are in their use subject to definite laws, partly agreeing with and partly differing from the laws of the corresponding symbols in the science of Algebra".*

Uma letra poderia representar o nome de alguma coisa, ou alguma qualidade ou circunstância relacionada a ela. Por exemplo, x sozinho poderia representar "coisas brancas", y sozinho "ovelha" e xy representaria "ovelha branca". Boole concluiu que a ordem em que os dois símbolos são escritos é indiferente, isto é, xy = yx. E se os dois símbolos têm o mesmo significado, sua combinação não expressa nada mais do que um deles sozinho, isto é, xy = x, o que nos leva a xx = x. Segue então que os símbolos da Lógica obedecem à lei especial

$$x^2 = x \qquad (1)$$

[5] Segundo J. L. Bell, Bertrand Russell observou certa vez que Boole descobriu a Matemática Pura [11].

A grande inovação de Boole é dada em seu passo seguinte, ao avaliar a última equação como uma equação algébrica, que admite apenas as raízes 0 e 1:

> *"Hence, instead of determining the measure of formal agreement of the symbols of Logic with those of Number generally, it is more immediately suggested to us to compare them with symbols of quantity* admitting only the values 0 and 1. *Let us conceive, then, of an Algebra in which the symbols x, y, z, &c. admit indifferently of the values 0 and 1, and of these values alone. The laws, the axioms, and the processes, of such an Algebra will be identical in their whole extent with the laws, the axioms, and the processes of an Algebra of Logic. Difference of interpretation will alone divide them. Upon this principle the method of the following work is established"*.

As interpretações dadas por Boole aos símbolos 0 e 1 são o *Nada* e o *Universo*, respectivamente. A partir disso, conclui que 1 – x representa a classe suplementar ou contrária da classe representada por x. Portanto, escrevendo (1) na forma $x - x^2 = 0$, segue-se que $x(1 - x) = 0$, o que significa que o "Princípio da Contradição", considerada por Aristóteles como axioma fundamental de toda Filosofia, (cf. *Metaphysica* III, 3, [13]), é uma conseqüência de (1), denominada "Equação Fundamental do Pensamento".

1.1 - Abordagem algébrica para a Lógica

Podemos ver que a Lógica Matemática é em suas origens notadamente algébrica e, em particular, a abordagem de Boole é essencialmente polinomial, ver [32], [33] e [34]. Muitos problemas encontrados por ele poderiam ser solucionados se trabalhasse com polinômios sobre Corpos de Galois.[6]

Não é necessário discutir os bem conhecidos progressos posteriores na Lógica Clássica, as origens das Lógicas Não-Clássicas e a aplicabilidade destas na Ciência da Computação, na Inteligência Artificial, na Lingüística, nas Ciências Cognitivas, em todo tipo de tecnologias, etc.

A abordagem algébrica tem se mostrado muito fértil no tratamento de problemas da Lógica. Para citar apenas um exemplo, o próprio Łukasiewicz introduz as Lógicas Polivalentes de forma essencialmente algébrica e tal é o tratamento dado por Chang, que

[6] Por exemplo, seria possível a generalização $x^n = x$, rejeitada por Boole.

introduz as MV-álgebras e chama a atenção sobre suas relações com a Teoria dos Grupos Abelianos Ordenados. Chang, utiliza métodos algébricos para a demonstração da completude dos Cálculos Infinitovalentes, ver [14] e [15].

As vantagens dos sistemas algébricos de prova têm despertado a atenção dos pesquisadores e, em especial, o emprego de anéis de polinômios sobre corpos de Galois parece bastante promissor, visto que além de resgatar o "espírito" original no estudo das Lógicas, também possibilita o desenvolvimento de procedimentos de prova automática e a investigação sobre a complexidade de algoritmos. Destaca-se o Cálculo com Anéis de Polinômios como método algébrico de prova, sobretudo por ser inovador no estudo das Lógicas Não-Clássicas. Apesar de resultados relacionados com os Cálculos Proposicionais, os Cálculos dos Anéis de Polinômios para as Lógicas de Primeira Ordem e de ordens superiores não foram suficientemente estudados.

2 - Universo de Discurso

Para maior clareza apresentamos, a seguir, os elementos básicos que formam o universo de discurso deste artigo e, tendo em vista que o método algébrico de prova por meio de Cálculo com Anéis de Polinômios é uma teoria nascente, apresentamos uma visão panorâmica sobre as principais idéias e resultados envolvidos.

2.1 - Elementos

2.1.1 - Relação de Conseqüência

Dada uma linguagem $\mathcal{L}$, uma *relação de conseqüência* é uma relação $\vdash \subseteq (\wp(\mathtt{For}) \times \mathtt{For})$, ou seja, uma relação $\vdash$ entre subconjuntos e elementos de $\mathtt{For}$. Os elementos de $\mathtt{For}$ são interpretados como *fórmulas* e os subconjuntos de $\mathtt{For}$ como *teorias*.

Uma relação $\vdash$ pode ser definida *sintaticamente*, por meio de axiomas específicos, ou *semanticamente*, por meio de uma interpretação semântica. Em geral $\vdash$ satisfaz as seguintes condições:

i. (Reflexividade) Se $A \in \Gamma$ então $\Gamma \vdash A$
ii. (Transitividade) Se $\Gamma \vdash A$ e $\Delta, A \vdash B$ então $\Gamma, \Delta \vdash B$
iii. (Monotonicidade) Se $\Gamma \vdash A$ e $\Gamma \subseteq \Delta$ então $\Delta \vdash A$
iv. (Estruturalidade) Se $\Gamma \vdash A$ então $\sigma(\Gamma) \vdash \sigma(A)$, para toda substituição σ
v. (Finitariedade) Se $\Gamma \vdash A$ então $\Delta \vdash A$, para algum conjunto finito $\Delta \subseteq \Gamma$

2.1.2 - Operadores de Conseqüência

Um *operador de conseqüência* é um operador de fecho Cl sobre um conjunto S de fórmulas, ou seja, $Cl : \wp(S) \rightarrow \wp(S)$, tal que para todo $X, Y \subseteq S$, vale:

i. (Extensividade) $X \subseteq Cl(X)$
ii. (Monotonia e/ou Isotonia) Se $X \subseteq Y$ então $Cl(X) \subseteq Cl(Y)$
iii. (Idempotência) $Cl(Cl(X)) = Cl(X)$

2.1.3 - Lógicas e Sistemas Dedutivos

Uma *Lógica* pode ser definida como um par $\mathbb{L} = \langle \mathcal{L}, Cl \rangle$, onde $\mathcal{L}$ é um conjunto não-vazio e Cl é um operador de conseqüência sobre $\mathcal{L}$. Um *sistema dedutivo* ou um *sistema lógico* $\mathfrak{S}$ é simplesmente uma estrutura $\mathfrak{S} = \langle For, \vdash \rangle$ (cf. [20]).

2.1.4 - Procedimentos de Cálculo com Anéis de Polinômios

Os Sistemas Algébricos de prova são sistemas que exploram métodos e resultados da Álgebra para expressar demonstrações. Tais sistemas podem ser aplicados em procedimentos de prova automática e em investigações acerca da complexidade de algoritmos.

O método das bases de Gröbner é um método algébrico bem conhecido. Este é fundamentado na Teoria dos Ideais e utiliza o Teorema do *Nullstellensatz* de Hilbert e foi introduzido por Buchberger em 1965, ver [16], [17], [18] e [19].

Dentre as pesquisas atuais, destaca-se o método algébrico mais simples e mais amplo denominado *Cálculo com Anéis de Polinômios* (*Polynomial Ring Calculus*,

PRC), proposto por Carnielli em [21], ver [22], [23] e [24]. Este faz uso da estrutura de corpos finitos (corpos de Galois) e, diferentemente do método das bases de Gröbner, pode englobar todas as lógicas multivalentes verofuncionais e uma significante classe de lógicas não-verofuncionais.

2.1.5 - Cálculo com Anéis de Polinômios

Seja $\mathbb{L}$ uma lógica p^n-valente e D o conjunto de valores-verdade de $\mathbb{L}$. A seguir descrevemos o *Cálculo com Anéis de Polinômios* (**PRC**).[7]

Definição 1. Seja $\langle \mathbf{F}, +, ., 0, 1 \rangle$ um anel abeliano com unidade 1 e zero 0. Seja $\mathbf{F}[X]$ o anel de todos os polinômios finitos nas variáveis $\vec{x} = x_1, x_2, ..., x_m, ...$ com grau arbitrário e característica p^n. Uma *proposição do Anel de Polinômios* para $\mathbb{L}$ ou simplesmente uma *proposição polinomial* é qualquer polinômio $f \in \mathbf{F}[X]$ sobre as variáveis $\vec{x}$.

Definição 2. Dada uma lógica $\mathbb{L}$, uma *interpretação polinomial* para $\mathbb{L}$ é uma interpretação $\Omega : \mathbb{L} \rightarrow \mathbf{F}[X]$, que associa a cada fbf φ um polinômio $\Omega(\varphi) \in \mathbf{F}[X]$.

Definição 3. Uma proposição polinomial f é *satisfazível* se existe uma valoração em $\mathbf{F}$ que produz $d \in D \subset \mathbf{F}$.

Notação: $f(\vec{x}) = d$ ou simplesmente $f = d$;

$f \approx g$ significa que $f = g$ para todas as valorações em $\mathbf{F}$;

$f \approx d$ $(d \in \mathbf{F})$ significa que f coincide com o polinômio constante d.

Observação:

Metavariáveis sobre variáveis: $x, y, z, ...,\ x_1, x_2, ...$

Metavariáveis sobre polinômios: $f, g, h, ...$

[7] As definições e resultados apresentados a seguir com poucas alterações são encontrados em [21] e [22].

Definição 4. Seja p um número primo e n um natural não-nulo. Define-se **(p,n)-PRC** para $\mathbb{L}$ sobre o corpo de Galois $\mathbf{GF}(p^n)$ do seguinte modo:

i. Os termos são as variáveis e as fórmulas são os polinômios de $\mathbf{GF}(p^n)[X]$;

ii. (Regras do Anel)

$\forall f, g, h \in \mathbf{GF}(p^n)[X]$ e $\vdash_{\approx} \subseteq (\wp(\mathbf{GF}(p^n)[X]) \times \mathbf{GF}(p^n)[X])$:

(a) $f + (g + h) \vdash_{\approx} (f + g) + h$
(b) $f + g \vdash_{\approx} g + f$
(c) $f + 0 \vdash_{\approx} f$
(d) $f + (-f) \vdash_{\approx} 0$
(e) $f \cdot (g \cdot h) \vdash_{\approx} (f \cdot g) \cdot h$
(f) $f \cdot (g + h) \vdash_{\approx} f \cdot g + f \cdot h$

(Regras Polinomiais):

(g) $p^n \cdot x = \underbrace{x + x + \ldots + x}_{p^n \text{ vezes}} \vdash_{\approx} 0$
(h) $x^i \cdot x^j \vdash_{\approx} x^k (\mathrm{mod}\, q(x))$,

para $k \equiv i + j (\mathrm{mod}(p^n - 1))$, onde $q(x)$ é um polinômio primitivo conveniente (i.e., um polinômio irredutível de grau n com coeficientes em $\mathbb{Z}_p$)

iii. (Meta-regras):

Substituição Uniforme (SU):

$$\frac{f \vdash_{\approx} g}{f[x : h] \vdash_{\approx} g[x : h]}$$

Regra de Leibniz (RL):

$$\frac{f \vdash_{\approx} g}{h[x : f] \vdash_{\approx} h[x : g]},$$

onde $f[x:g]$ denota o resultado da substituição uniforme de x por g em f.

A regra (SU) permite a substituição de todas as ocorrências de certa variável x no polinômio por outro polinômio e a regra (RL) permite a substituição de x em um polinômio por polinômios "equivalentes".

Se $\Delta \cup \{f\}$ é uma coleção de proposições polinomiais, uma derivação de f a partir de Δ, denotada por $\Delta \vdash_{\approx} f$, é uma seqüência finita de fórmulas polinomiais que ou estão em Δ ou são obtidas de fórmulas anteriores pela aplicação das regras de **(p,n)-PRC**. Se $\varnothing \vdash_{\approx} f$ então f é denominado um *teorema* e tal fato é denotado por $\vdash_{\approx} f$. Das aplicações das regras (SU) e (RL), obtém-se o seguinte resultado sobre a relação de conseqüência $\vdash_{\approx}$:

Teorema 5. As seguintes regras são derivadas, para qualquer conjunto de polinômios Δ e Σ e polinômios f, g e h:

1. $\Delta, f \vdash_{\approx} f$
2. Se $\Delta, f \vdash_{\approx} g$ e $\Sigma, g \vdash_{\approx} h$ então $\Delta, \Sigma, f \vdash_{\approx} h$
3. Se $\Delta, f \vdash_{\approx} g$ então $\Delta, \Sigma, f \vdash_{\approx} g$
4. Se $f \vdash_{\approx} 0$ então $g \cdot f \vdash_{\approx} 0$
5. Se $f \vdash_{\approx} g$ então $h \cdot f \vdash_{\approx} h \cdot g$ e $f \cdot h \vdash_{\approx} g \cdot h$
6. Se $f \vdash_{\approx} g$ então $h + f \vdash_{\approx} h + g$ e $f + h \vdash_{\approx} g + h$
7. Se $f \vdash_{\approx} 0$ e $g \vdash_{\approx} 0$ então $e \cdot f + h \cdot g \vdash_{\approx} 0$
8. $(n \cdot f) \vdash_{\approx} 0$ e $f^n \vdash_{\approx} f$. □

Para se definir um **PRC** para uma dada lógica $\mathbb{L}$ é necessária uma interpretação $\Omega : \mathbb{L} \rightarrow \mathbf{GF}(p^n)[X]$ de fórmulas em polinômios de modo que sejam preservadas as condições de uma classe de valorações para $\mathbb{L}$.

2.1.6 - Um Cálculo com Anel de Polinômios para a Lógica Proposicional Clássica

Como exemplo de um **PRC** para uma lógica particular, consideraremos a seguir a *Lógica Proposicional Clássica* (**LPC**).

Seja For o conjunto de fbf's de **LPC** sobre o alfabeto $\{\neg, \vee, \wedge\}$ e sejam as metavariáveis sobre fórmulas representadas por A, B, C, etc. Uma valoração para **LPC** é a função $v: For \rightarrow \{0, 1\}$ tal que

(2.1) $v(\neg A) = 1$ see $v(A) = 0$

(2.2) $v(A \vee B) = 1$ see $v(A) = 1$ ou $v(B) = 1$

(2.3) $v(A \wedge B) = 1$ see $v(A) = 1$ e $v(B) = 1$

Seja a interpretação booleana dada pela interpretação polinomial Ω **:LPC**$\rightarrow \mathbb{Z}_2[X]$, definida por

(2.4) $\Omega(p_i) \coloneqq x_i$ se p_i é uma variável proposicional

(2.5) $\Omega(\neg A) \coloneqq \Omega(A) + 1$

(2.6) $\Omega(A \vee B) \coloneqq \Omega(A) \cdot \Omega(B) + \Omega(A) + \Omega(B)$

(2.7) $\Omega(A \wedge B) \coloneqq \Omega(A) \cdot \Omega(B)$

Das regras polinomiais sobre $\mathbb{Z}_2[X]$, temos que

(2.8) $x + x \vdash_{\approx} 0$

(2.9) $x \cdot x \vdash_{\approx} x$

Se um polinômio $f \in \mathbb{Z}_2[X]$ é tal que $f \approx c \in \{0, 1\}$, então é possível verificar que após um número finito de sucessivas aplicações de (2.8) e (2.9) obtém-se $f \vdash_{\approx} c$ e vice-versa.

Generalizando tal fato, obtemos o seguinte resultado:

Teorema 6. Seja $f \in$ **GF**$(p^n)[X]$. Tem-se que $f \approx c \in D \subset$ **GF**(p^n) see $f \vdash_{\approx} c$ em **(p,n)-PRC**. □

Atribuindo-se os valores 0 ou 1 para as variáveis em X, verifica-se que Ω preserva as valorações de **LPC**, pois

(2.10) $\Omega(\neg A) \vdash_{\approx} 1$ see $\Omega(A) \vdash_{\approx} 0$

(2.11) $\Omega(A \vee B) \vdash_{\approx} 1$ see $\Omega(A) \vdash_{\approx} 1$ ou $\Omega(B) \vdash_{\approx} 1$

(2.12) $\Omega(A \wedge B) \vdash_{\approx} 1$ see $\Omega(A) \vdash_{\approx} 1$ e $\Omega(B) \vdash_{\approx} 1$.

Segue, como corolário do teorema anterior:

Teorema 7. Seja $\Omega\left(A(p_1,\ldots,p_k)\right) = f(x_1,\ldots,x_k)$. Tem-se que $f(x_1,\ldots,x_k)\approx 1$, $\forall\,(x_1,\ldots,x_k)\in\mathbb{Z}_2^k$, see $\vdash_{LPC} A(p_1,\ldots,p_k)$.□

Utilizando tal teorema exibimos dois exemplos de provas polinomiais de teoremas de **LPC**:

(a) $\vdash_{LPC} A \rightarrow A$, para toda fbf A.

Prova

De (2.5) e (2.6), temos:

$$\begin{aligned}\Omega(A \rightarrow A) &= \Omega(A)\cdot\Omega(A) + \Omega(A) + 1 \approx\\ &\approx \Omega(A) + \Omega(A) + 1 \approx\\ &\approx 0 + 1 \approx\\ &\approx 1.\end{aligned}$$

(b) $\vdash_{LPC} \neg\neg A \rightarrow A$, para toda fbf A.

Prova

$$\begin{aligned}\Omega(\neg\neg A \rightarrow A) &= \Omega(\neg\neg A)\cdot\Omega(A) + \Omega(\neg\neg A) + 1 =\\ &= \left(\Omega(\neg A) + 1\right)\cdot\Omega(A) + \left(\Omega(\neg A) + 1\right) + 1 =\\ &= \left(\left(\Omega(A) + 1\right) + 1\right)\cdot\Omega(A) + \left(\left(\Omega(A) + 1\right) + 1\right) + 1 \approx\\ &\approx \left(\Omega(A) + (1 + 1)\right)\cdot\Omega(A) + \left(\Omega(A) + (1 + 1)\right) + 1 \approx\\ &\approx \left(\Omega(A) + 0\right)\cdot\Omega(A) + \left(\Omega(A) + 0\right) + 1 \approx\\ &\approx \Omega(A)\cdot\Omega(A) + \Omega(A) + 1 \approx\\ &\approx \Omega(A) + \Omega(A) + 1 \approx\\ &\approx 0 + 1 \approx\\ &\approx 1.\end{aligned}$$

Se a valoração $v: For \to \{0, 1\}$ for expandida para uma função $v': For \to [0, 1]$, a mesma interpretação polinomial Ω, juntamente com as aplicações das regras de **RPC** o resultado é uma Lógica Polinomial Minimal (*Minimal Polynomial Logic*, MPL), introduzida por Poli *et al*., ver [28], cujas possíveis semânticas são similares a Lógica Probabilística de Nilsson [26] e [27] ou a Lógica Fuzzy [29], [30] e [31].

2.1.7 - Lógicas de Łukasiewicz na forma polinomial

Como um exemplo particular da aplicação de **RPC** para as Lógicas de Łukasiewicz, apresentamos a interpretação polinomial para o cálculo proposicional da lógica trivalente $\mathbf{Ł_3}$:

Seja For o conjunto de fbf's dos cálculos proposicionais de Łukasiewicz ($\mathbf{Ł_n}$) sobre o alfabeto $\{\neg, \to\}$ e sejam as metavariáveis sobre fórmulas representadas por A, B, C, etc.

Uma valoração das fórmulas no intervalo $[0, 1]$ é uma função $v: For \to [0, 1]$ tal que

$$v(\neg A) = \neg v(A) \tag{2.13}$$

$$v(A \to B) = v(A) \to v(B), \tag{2.14}$$

onde para $x, y \in [0, 1]$,

$$\neg x := 1 - x \quad e \quad x \to y := \min(1, 1 - x + y). \tag{2.15}$$

Para $\mathbf{Ł_3}$, $D = \left\{0, \frac{1}{2}, 1\right\} \subset [0, 1]$ e as tabelas-verdade de $\neg$ e $\to$ são:

x	$\neg x$
0	1
1/2	1/2
1	0

$x \to y$

x\y	0	1/2	1
0	1	1	1
1/2	1/2	1	1
1	0	1/2	1

Utilizando a bijeção $t: \left\{0, \frac{1}{2}, 1\right\} \to \{0, 1, 2\}$ dada por $t(0) = 0$, $t(1/2) = 1$ e $t(1) = 2$, obtemos as seguintes tabelas-verdade:

X	¬x
0	2
1	1
2	0

$x \to y$

x\y	0	1	2
0	2	2	2
1	1	2	2
2	0	1	2

Uma interpretação polinomial $\Omega : \mathbb{L}_3 \to \mathbb{Z}_3[X]$, é definida por:

$$(2.16)\ \Omega(\neg A) := 2 \cdot \Omega(A) + 2$$

$$(2.17)$$

$$\Omega(A \to B) := 2 \cdot \Omega(A) \cdot (\Omega(B) + 1) \cdot (\Omega(A) \cdot \Omega(B) + \Omega(B) + 1) + 2$$

Logo, para $x, y \in \{0, 1, 2\}$ a interpretação polinomial dos conectivos $\neg$ e $\to$ são:

$$(2.18) \qquad \neg x = 2x + 2 \ \text{ e } \ x \to y = 2x(y + 1)(xy + y + 1) + 2.$$

O conectivo $\oplus$ é dado por $x \oplus y = \neg x \to y$. Como exemplo, consideremos a prova polinomial de $A \oplus \neg A$:

Das regras polinomiais, temos que $3x = 0$ e $x^3 = x$, logo

$$x \oplus \neg x = \neg x \to \neg x = (2x + 2) \to (2x + 2) =$$

$$= 2(2x + 2)(2x + 2 + 1)\left((2x + 2)^2 + 2x + 2 + 1\right) + 2 =$$

$$= (4x + 4)2x\left(4x^2 + 8x + 4 + 2x\right) + 2 =$$

$$= (x + 1)2x\left(x^2 + 2x + 1 + 2x\right) + 2 =$$

$$= \left(2x^2 + 2x\right)\left(x^2 + x + 1\right) + 2 =$$

$$= 2x^4 + 2x^3 + 2x^2 + 2x^3 + 2x^2 + 2x + 2 =$$
$$= 2x^2 + 2x + 2x^2 + 2x + 2x^2 + 2x + 2 =$$
$$= 6x^2 + 6x + 2 = 2$$

Pelo Teorema 2.5 em [21], temos que $\vdash_{Ł_3PC} A \oplus \neg A$.

Outros exemplos de aplicações, como para Lógica Paraconsistente *mbC*, a Teoria dos silogismos, etc, podem ser vistos em [21], [22] e [23] e [24].

2.1.8 - Lógica de Primeira Ordem e Polinômios Infinitos

Os exemplos considerados e explorados limitam-se aos Cálculos Proposicionais, estando em aberto as extensões deste método algébrico do **RPC** para as Lógicas quantificadas. No caso da Lógica de Primeira Ordem (**FOL**), como sugere Carnielli em [21], a interpretação polinomial de **LPC** pode ser expandida para uma interpretação Ω : **FOL** $\rightarrow \mathbb{Z}_2[X]$, de modo que

i. Para cada constante c_i, $\Omega(A(c_i)) = x_i^A$

ii. $\Omega(\forall z A(z)) = \prod_{i=1}^{\infty} x_i^A$.

De (i) temos que cada $A(c_i)$ é interpretado como uma nova variável em $\mathbb{Z}_2$ e de (ii), temos que $\Omega(\exists z A(z)) = \Omega(\neg\forall z \neg A(z)) = 1 + \prod_{i=1}^{\infty}(1 + x_i^A)$.

Interpretar fórmulas quantificadas em **FOL** (ou em Lógicas de ordem superior) como séries formais reduz as técnicas de prova a um ramo da Análise Funcional.

3 - Problemas em aberto e possíveis perspectivas

Baseado nas ideias acima expostas, apresenta-se a necessidade de se desenvolver um Cálculo com Anel de Polinômios para a Lógica de Primeira Ordem, bem como as

possíveis extensões para Lógicas de ordem superior. Um possível caminho seria por meio de um estudo das relações entre **RPC** e a Análise Funcional.

Como a Completude da **LPC** é equivalente ao Axioma da Escolha, em termos de Anéis de Polinômios, deve ser equivalente a algum resultado da Análise. Carnielli conjecturou, conforme comunicação pessoal, que a Completude de **LPC** esteja relacionada com alguma variação do Teorema de Hahn-Banach, que mostra que todos funcionais lineares definidos em um subespaço de determinado espaço vetorial podem ser estendidos a todo o espaço. Portanto, é de grande interesse o estudo do(s) possível(is) princípio(s) de polinômios que garantem a Completude da Lógica de Primeira Ordem, no referido contexto.

Em recente tese de Doutoramento junto à Universidade Estadual de Campinas (2013, [35]), Mariana Matulovic, sob orientação de Carnielli, definiu uma versão da Lógica de Primeira Ordem (**LPO**) nas formas sintática e semântica, supondo que a noção de consequência sintática seja caracterizada pela noção de consequência semântica. Define um domínio de séries formais generalizadas por produtos (**SGP**), que generaliza a noção de polinômios finitos e infinitos. Deste modo, torna-se possível traduzir as fórmulas da **LPO** em **SGP**, na qual se reduz a satisfatibilidades lógica à prova finitária, com elementos infinitos. Como a **LPO** considerada é correta e completa, conclui-se que a derivabilidade lógica é caracterizada pela solubilidade algébrica em **SGP**. Deste modo, Matulovic define a **LPO** em uma versão polinomial (ou polinômica) e demonstra os teoremas de correção e completude (fraca e forte) para o sistema.[8]

[8] Gostaria de expressar meus sinceros agradecimentos a Walter Carnielli e a Mariana Matulovic pelas informações sobre os mais recentes resultados na referida área de investigação. Registre-se, todavia, que quaisquer imprecisões na exposição devem ser a mim imputadas. Segue uma sinopse da tese de Matulovic:
Capítulo 1: Apanhado histórico acerca do desenvolvimento dos polinômios, culminando com uma análise sobre as inter-relações entre lógica e álgebra e, consequentemente, sobre a algebrização da lógica. Além disso, introduz-se os conceitos primordiais a respeito do método de anéis de polinômios e são delineamos alguns dos resultados já obtidos na aplicação do método ao Cálculo Proposicional Clássico e ao fragmento monádico da Lógica de Primeira Ordem.
Capítulo 2: Dedicado às Lógicas da Inconsistência Formal (**LFIs**) e alguns avanços no já obtido por Carnielli para as lógicas mbC e mCi, definindo versões polinômicas para as seguintes **LFIs**: bC, Ci, mbCe, mCie, bCe, Cie e LFI1. Ademais, apresenta-se algumas melhorias as apresentações polinomiais para os sistemas mbC e mCi.
Capítulo 3: Aplicabilidade no método de anéis de polinômios em sistemas lógicos cujas semânticas são não-determinísticas.
Capítulo 4: Investigação da perda da verofuncionalidade em sistemas n-valorados que foram reduzidos em bivalorados, pela chamada Redução de Suszko.
Capítulo 5: Definição da 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 permite operar com somas e produtos infinitos.

Evidencia-se deste modo, a riqueza de possibilidades que o Método de Cálculo com Anel de Polinômios propicia para o estudo e análise de diversos problemas em Lógica e Matemática.

4 - Referências Bibliográficas

[1] BERTATO, Fábio Maia; D'OTTAVIANO, Itala M. Loffredo. Luca Pacioli and the "Controversy of the Perspective": the classification of the mathematics from the classical antiquity to the end of the quattrocento. **Revista Brasileira de História da Matemática,** Rio Claro, Especial nº 1, - Festschrift Ubiratan D'Ambrosio, p. 505-525, dez. 2008.
[2] BERTATO, Fábio Maia. **A "De Divina Proportione" de Luca Pacioli - Tradução Anotada e Comentada.** xlivp., 292p. Tese de Doutorado (Filosofia). Instituto de Filosofia e Ciências Humanas, Universidade Estadual de Campinas. Campinas, 2008.
[3] BERTATO, Fábio Maia. **A "De Divina Proportione" de Luca Pacioli - Tradução Anotada e Comentada.** Campinas: Coleção CLE, 2010, v. 56, 344p.
[4] D'OTTAVIANO, Itala M. Loffredo; FEITOSA, Hércules. A. **História da lógica e o surgimento das lógicas não clássicas.** Coleção História da Matemática para Professores, SBHM/UNESP, v. 1, p. 01-66, 2003.
[5] GOLDSTEIN, Rebecca. **Incompletude: a prova e o paradoxo de Kurt Gödel.** Trad. Ivo Korytowski. São Paulo: Companhia das Letras, 2008.
[6] BUSCHE, Hubertus. **Leibniz' Weg ins perspektivische Universum: eine Harmonie im Zeitalter der Berechnung.** Hamburg: Felix Meiner Verlag, 1997.
[7] CARRUCCIO, Ettore; **Mathematics and Logic in History and in Contemporary Thought.** Trad. Isabel Quigly. Chicago: Aldine Transaction, 2006.
[8] PEACOCK, George. **Treatise on Algebra**. 1845.
[9] KATZ, Victor J. **A History of Mathematics: An Introduction.** New York: HarperCollins, 1993.
[10] DE MORGAN, Augustus. **Trigonometry and Double Algebra.** London: Taylor, 1849.
[11] SLOMSON, A. B.; BELL, J. L. **Models and Ultraproducts: An Introduction.** Amsterdam: North-Holland, 1969.
[12] BOOLE, George. **An investigation of the laws of thought: on which are founded the mathematical theories of logic and probabilities.** London: Walton and Maberly, 1854.
[13] ARISTÓTELES. YEBRA, Valentín Garcia (ed.). **Metafísica.** Madrid: Editorail Gredos, 1970. v.1. (Edição Trilíngüe: Grego, Latim e Espanhol).
[14] CIGNOLI, Roberto. L. O.; D'OTTAVIANO, Itala. M. L.; MUNDICI, Daniele. **Algebraic foundations of many-valued reasoning.** Dordrecht: Kluwer Academic Publishers, 2000. v. 2.
[15] CIGNOLI, Roberto. L. O.; D'OTTAVIANO, Itala. M. L.; MUNDICI, Daniele. **Álgebras das lógicas de Lukasiewicz.** Coleção CLE, v. 12, (2ª Ed.). Campinas: CLE/UNICAMP, 1995.
[16] BUCHBERGER, Bruno. **Ein Algorithmus zum Auffinden der Basiselemente des Restklassenriges nach einem nulldimensionalen Polynomideal.** Tese de doutorado (Filosofia). Universität Innsbruck. Innsbruck, 1965.

[17] BUCHBERGER, Bruno. An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal. Trad. por M. Abramson in **Journal of Symbolic Computation** 41 (2006): 471-511.
[18] BUCHBERGER, Bruno. Ein algorithmisches Kriterium für die Lösbrakeit eines algebraischen Gleichungssystems. **Aequationes Mathematicae 4** (1970): 374-383.
[19] BUCHBERGER, Bruno; WINKLER, F. (eds.). Gröbner Bases and Applications. Trad. por M. Abramson e Robert Lumbert. **London Mathematical Society Lecture Note Series 251**, Cambridge University Press, 1998, 535-545.
[20] D'OTTAVIANO, Itala M. L. ; FEITOSA, Hércules A. . Deductive systems and translations. In: Jean-Yves Béziau; Alexandre Costa-Leite. (Org.). **Perspectives on Universal Logic.** 1 ed. Itália: Polimetrica International Scientific Publisher, 2007, v. , p. 125-157.
[21] CARNIELLI, Walter A.. Polynomial ring calculus for many-valued logics. In B. Werner (ed.). **Proceedings of the 35th International Symposium on Multiple-Valued Logic.** Calgary, Canadá: IEEE Computer Society, 2005. P. 20-25.
[22] CARNIELLI, Walter A.. Polynomizing: Logic Inference in Polynomial Format and the Legacy of Boole. **Studies in Computational Intelligence.** Vol. 64, p. 349-364, 2007.
[23] AGUDELO, Juan C.; CARNIELLI, Walter A.. Unconventional models of computation through non-standard logic circuits. **Lecture Notes in Computer Science**. Vol. 4618. Berlin: Springer, p 29-40, 2007.
[24] AGUDELO, Juan C.; CARNIELLI, Walter A.. Polynomial ring calculus for modal logics: a new semantics and proof method for modalities. **CLE e-Prints.** Vol.9(4), 2009.
[25] CORCORAN, John. Aristotle's Prior Analytics and Boole's Laws of Thought. **History and Philosophy of Logic 24,** p.261-288, 2003.
[26] NILSSON, N. J.. Probabilistic logic. **Artificial Intelligence.** Vol. 28(1), p 71-87, 1986.
[27] NILSSON, N. J.. Probabilistic logic revisited. **Artificial Intelligence.** Vol. 59(1), p.39-42, 1993.
[28] POLI, R.; RYAN, M.; SLOMAN, A.. A new continuous propositional logic. In C. Pinto-Ferreira and N. J. Mamede (ed.). **Proceedings of 7th Portuguese Conference on Artificial Intelligence**. Madeira Island: EPIA '95, 990 in Lecture Notes in Artificial Intelligence Funchal, 1995. p. 17-28.
[29] NGUYEN, Hung T.; WALKER, Elbert. **A first course in fuzzy logic.** CRC Press. 2006.
[30] HÁJEK, Petr. **Metamathematics of Fuzzy Logic.** Berlin: Springer. 1998.
[31] ZIMMERMANN, Hans-Jürgen. **Fuzzy Set Theory and Its Applications.** Berlin: Springer. 2001.
[32] HALMOS, Paul; GIVANT, Steven. Logic as Algebra. **Dolciani Mathematical Expositions 21.** The Mathematical Association of America. 1998.
[33] RICHE, Jacques. From Universal Algebra to Universal Logic. In: Jean-Yves Béziau; Alexandre Costa-Leite (eds.). **Perspectives on Universal Logic.** Itália: Polimetrica Publisher. p.3-39, 2007.
[34] JENSEN, Christian U.; LENZING, Helmt. Model Theoretic Algebra: with Particular Emphasis on Fields, Rings, Modules. **Algebra, Logic and Applications.** Vol. 2. Amsterdan: Gordon and Breach Science Publishers, 1989.
[35] MATULOVIC, Mariana. **Demonstrações na Algibeira: Polinômios como um Método Universal de Prova.** Campinas, SP: [s.n.], 2013. Orientador: Walter Alexandre

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