TEORIA DA PROVA

MARIA DA PAZ NUNES DE MEDEIROS
UFRN

1. Introdução

A expressão *teoria da prova*, uma tradução da expressão alemã *beweis-theorie*, foi introduzida por Hilbert e denomina hoje um importante ramo da lógica cujo objetivo principal é tratar provas como objeto de investigação. A sua origem está associada ao Programa de Hilbert desenvolvido no início do século XX, que consistia em explorar a natureza finitista das provas para fornecer uma fundamentação para a matemática. Neste programa, Hilbert buscava uma completa formalização da matemática, especialmente da aritmética e da análise, com o objetivo de evitar os paradoxos que surgiram na teoria do conjuntos e estavam fortemente relacionados ao conceito de infinito.

Sabidamente, com os teoremas de incompletude de Gödel apresentados em 1931, que tratavam da incompletude da aritmética e da impossibilidade de demonstrar a consistência da aritmética usando a própria aritmética, veio a tona a impossibilidade da completa realização do programa de Hilbert. Na demonstração destes teoremas, Gödel apresentou pela primeira vez a formalização do conceito "ser demonstrável na aritmética", que é considerada o ponto de partida do que posteriormente foi chamado de Lógica da Provabilidade, um importante ramo da Teoria da prova que apresentaremos posteriormente.

Sem dúvida alguma, um marco decisivo no desenvolvimento da Teoria da prova deve ser atribuído à Gentzen. Também preocupado com questões relativas aos fundamentos da aritmética, Gentzen apresentou em 1935 duas novas formulações para a lógica clássica de predicados de primeira ordem denominadas Dedução natural, **NK**, e Cálculo de seqüentes, **LK**, que tinham a vantagem de expressar as deduções lógicas de forma muito mais próxima ao raciocínio matemático do que os já conhecidos sistemas hilbertianos. Além disso, Gentzen mostrou que toda derivação do sistema **LK** poderia ser transformada em uma derivação que não é redundante no sentido que os únicos conceitos envolvidos ao longo dessa derivação são essenciais para a obtenção do resultado final. Este resultado foi chamado de Teorema de eliminação do corte (*Hauptsatz*), uma das principais motivações de Gentzen para a sua posterior demonstração da consistência da aritmética. Muitas variantes aos sistemas de Gentzen têm sido propostas. Nas seções 2 e

3 apresentaremos com mais detalhes uma formulação em dedução natural e uma em cálculo de seqüentes, respectivamente, para a lógica de predicados de primeira ordem.

Os estudos recentes em Teoria da prova extrapolam o domínio matemático filosófico e estão fortemente relacionado à Ciência da computação na medida em que buscam extrair informações construtivas ou computacionais de provas matemáticas, possibilitando uma melhor conexão entre provas e programas. Estas e outras discussões sobre problemas abertos na área de Teoria da prova podem ser encontrados em www.logic.stanford.edu/proofsurvey.html.

2. Dedução Natural

O sistema em Dedução natural para o cálculo de predicados de primeira ordem que vamos apresentar é a versão desenvolvida por Prawitz [7], denominada **C**, com pequenas modificações de ordem notacional.

A linguagem de **C** é constituída pelo conjunto $\{\rightarrow, \wedge, \vee, \forall, \exists, \bot\}$ de símbolos lógicos, além dos usuais símbolos não lógicos.
Símbolo definido: $\sim A =_{def} (A \rightarrow \bot)$

Regras de inferência para **C**:

$$(I\rightarrow)\quad \frac{\begin{array}{c}[A]^i\\ \vdots\\ B\end{array}}{A\rightarrow B}\,i \qquad (E\rightarrow)\quad \frac{A \qquad A\rightarrow B}{B}$$

$$(I\wedge)\quad \frac{A \qquad B}{A\wedge B} \qquad (E\wedge)\quad \frac{A\wedge B}{A} \qquad \frac{A\wedge B}{B}$$

$$(I\vee)\quad \frac{A}{A\vee B} \qquad \frac{B}{A\vee B} \qquad (E\vee)\quad \frac{A\vee B \quad \begin{array}{c}[A]^i\\ \vdots\\ C\end{array} \quad \begin{array}{c}[B]^j\\ \vdots\\ C\end{array}}{C}\,i,j$$

$$(I\forall)\quad \frac{A(x/y)}{\forall x A} \qquad (E\forall)\quad \frac{\forall x A}{A(x/t)}$$

$$(I\exists)\quad \frac{A(x/t)}{\exists x A} \qquad (E\exists)\quad \frac{\exists x A \qquad \begin{array}{c}[A(x/y)]^i\\ \vdots\\ B\end{array}}{B}\,i$$

$$(\bot_c)\quad \frac{\begin{array}{c}[\sim A]^i\\ \vdots\\ \bot\end{array}}{A}\,i$$

Restrições:
i) na regra $(I\forall)$, a variável y não deve ocorrer livre em uma hipótese da qual A dependa,
ii) na regra $(E\exists)$, y não deve ocorrer livre em $\exists xA$, em B, nem em qualquer hipótese da qual a conclusão B dependa.

Em cada regra de inferência as fórmulas imediatamente acima do traço horizontal são chamadas *premissas* e a imediatamente abaixo de *conclusão*. Nas regras $(I\rightarrow)$, $(E\vee)$, $(E\exists)$ e $(\perp_c)$, $[A]^i$ e $[B]^j$, significam o conjunto das hipóteses descarregadas em função de aplicações dessas regras. Os índices i e j indicam em que aplicações tais hipóteses são descarregadas. A expressão $A(x/t)$ denota o resultado de substituir todas as ocorrências livres da variável x pelo termo t na fórmula A.

Uma *derivação* no sistema **C** é um encadeamento de aplicações de regras de inferência em forma de árvore (figura de prova) cujos nós são fórmulas. Mais precisamente, se Π_1,... Π_n, $0 \leq n \leq 3$, são derivações e r uma aplicação de uma regra de inferência, então

$$\frac{\Pi_1, ...\Pi_n}{A}\, r$$

é uma derivação.

Observamos que com exceção do símbolo $\perp$, a cada símbolo lógico são associados duas regras de inferência: uma de introdução e outra de eliminação. As regras de introdução, $\{I\rightarrow, I\wedge, I\vee, I\forall, I\exists\}$, permitem para cada símbolo lógico a inferência de uma fórmula cujo símbolo principal é o símbolo em questão, enquanto que as regras de eliminação, $\{E\rightarrow, E\wedge, E\vee, E\forall, E\exists\}$, permitem retirar consequências das afirmações das premissas da regra indicada. Por exemplo, a regra de introdução para o símbolo $\wedge$ nos permite inferir a fórmula $(A \wedge B)$ a partir das premissas A e B. Igualmente, podemos introduzir a fórmula $(A \rightarrow B)$, se existe uma derivação de B a partir de A. Por outro lado, a regra de eliminação para o símbolo $\rightarrow$ permite inferir a fórmula B a partir das fórmulas A e $(A \rightarrow B)$. Desse modo, as regras de introdução e eliminação possibilitam o processo de composição e decomposição, respectivamente, de fórmulas em uma derivação. As fórmulas geradas a partir do processo de decomposição são chamadas *subfórmulas*.

A regra $(\perp_c)$, chamada *absurdo clássico*, representa a principal diferença entre o sistema **C** de Prawitz e o originalmente apresentado por Gentzen [4]. Lembramos que no sistema **NK**, Gentzen introduziu a fórmula $(A\vee \sim A)$ como axioma para que seu sistema fosse dedutivamente equivalente aos sistemas clássicos de primeira ordem já conhecidos.

Se eliminarmos a regra $(\perp_c)$ do sistema **C**, o fragmento resultante é logicamente equivalente à Lógica minimal, e se substituirmos a regra $(\perp_c)$ pela regra *absurdo intuicionista*,

$$(\perp_I) \quad \frac{\perp}{A}\,,$$

obteremos em dedução natural o correspondente à Lógica intuicionista.

Uma propriedade desejável a qualquer sistema em dedução natural é que ele satisfaça o Teorema de normalização. A primeira prova de normalização foi desenvolvida por Prawitz [7] para o fragmento $\{\wedge, \rightarrow, \bot, \forall\}$ da lógica clássica de primeira ordem, $\mathbf{C}'$, um sistema dedutivamente equivalente a $\mathbf{C}$. Para melhor compreendermos o que significa tudo isso, vejamos algumas definições preliminares.

As premissas $(A \rightarrow B)$, $(A \wedge B)$, $(A \vee B)$, $\forall x A$ e $\exists x A$ que ocorrem nas regras de eliminação são chamadas de *premissa maior*, as demais de *premissa menor*. Uma fórmula A é chamada *máxima* em uma derivação, se A é ao mesmo tempo conseqüência de uma aplicação de uma regra de introdução ou $(\bot_c)$ e premissa maior de uma aplicação de uma regra de eliminação. Uma *derivação normal* em $\mathbf{C}'$ é uma derivação que não tem ocorrência de fórmulas máximas.

O Teorema de normalização assevera que toda derivação do sistema $\mathbf{C}'$ pode ser transformada em uma derivação normal. A sua demonstração segue de um resultado preliminar que garante que toda aplicação da regra de absurdo clássico neste fragmento pode ser reduzida a fórmulas atômicas.

Como conseqüência imediata do Teorema de normalização tem-se o Princípio de subfórmula: toda ocorrência de uma fórmula em uma derivação normal de A a partir de um conjunto Γ de fórmulas em $\mathbf{C}'$ é uma subfórmula de A ou de alguma fórmula de Γ com exceção das hipóteses descarregadas por aplicações de $(\bot_c)$ e das ocorrências de $\bot$ que estão imediatamente abaixo de tais hipóteses.

Já existem provas de normalização para sistemas clássicos em dedução natural que consideram o conjunto completo de conectivos e quantificadores lógicos. Podemos citar por exemplo a prova apresentada por Pereira e Massi [6].

3. Cálculo de sequentes

Gentzen [4] desenvolveu o Cálculo de seqüentes para a lógica de predicados de primeira ordem com o objetivo de obter um sistema lógico cujas formas de inferência possibilitassem a introdução e eliminação de todos os símbolos lógicos, sem perder a simetria das regras lógicas e além disso, que suas derivações fossem normalizáveis. Gentzen introduziu um novo conceito chamado *seqüente*, que tem a forma

$$A_1, ..., A_n \Rightarrow B_1, ..., B_m$$

e tem como interpretação a fórmula $(A_1 \wedge ... \wedge A_n \rightarrow B_1 \vee ... \vee B_m)$. Neste seqüente, a seqüência de fórmulas $A_1, ..., A_n$ é chamada *antecedente* do seqüente e a seqüência $B_1, ..., B_m$ de *conseqüente* do seqüente. Ambos podem ser eventualmente vazios.

Apresentaremos um sistema em Cálculo de seqüentes, **CS**, para a lógica clássica de predicados de primeira ordem que difere do sistema **LK** de Gentzen apenas quanto a notação.

A linguagem de **CS** é constituída pelo conjunto $\{\rightarrow, \wedge, \vee, \forall, \exists, \sim\}$ de símbolos lógicos, além dos usuais símbolos não lógicos. Usaremos as letras Γ e Δ, com ou sem índices, para representar seqüências finitas de fórmulas.

Seqüente inicial: $A \Rightarrow A$

Regras lógicas:

$$(L\wedge)\quad \frac{A, B, \Gamma \Rightarrow \Delta}{A \wedge B, \Gamma \Rightarrow \Delta} \qquad (R\wedge)\quad \frac{\Gamma_1 \Rightarrow \Delta, A \quad \Gamma_2 \Rightarrow \Delta, B}{\Gamma_1, \Gamma_2 \Rightarrow \Delta, A \wedge B}$$

$$(L\vee)\quad \frac{A, \Gamma_1 \Rightarrow \Delta \quad B, \Gamma_2 \Rightarrow \Delta}{A \vee B, \Gamma_1, \Gamma_2 \Rightarrow \Delta} \qquad (R\vee)\quad \frac{\Gamma \Rightarrow \Delta, A, B}{\Gamma \Rightarrow \Delta, A \vee B}$$

$$(L\rightarrow)\quad \frac{\Gamma_1 \Rightarrow \Delta_1, A \quad B, \Gamma_2 \Rightarrow \Delta_2}{A \rightarrow B, \Gamma_1, \Gamma_2 \Rightarrow \Delta_1, \Delta_2} \qquad (R\rightarrow)\quad \frac{A, \Gamma \Rightarrow \Delta, B}{\Gamma \Rightarrow \Delta, A \rightarrow B}$$

$$(L\sim)\quad \frac{\Gamma \Rightarrow \Delta, A}{\sim A, \Gamma \Rightarrow \Delta} \qquad (R\sim)\quad \frac{A, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \sim A}$$

$$(L\forall)\quad \frac{A(x/t), \Gamma \Rightarrow \Delta}{\forall x A, \Gamma \Rightarrow \Delta} \qquad (R\forall)\quad \frac{\Gamma \Rightarrow \Delta, A(x/y)}{\Gamma \Rightarrow \Delta, \forall x A}$$

$$(L\exists)\quad \frac{A(x/y), \Gamma \Rightarrow \Delta}{\exists x A, \Gamma \Rightarrow \Delta} \qquad (R\exists)\quad \frac{\Gamma \Rightarrow \Delta, A(x/t)}{\Gamma \Rightarrow \Delta, \exists x A}$$

Regras estruturais:

$$(LW)\quad \frac{\Gamma \Rightarrow \Delta}{A, \Gamma \Rightarrow \Delta} \qquad (RW)\quad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, A}$$

$$(LP)\quad \frac{\Gamma_1, A, B, \Gamma_2 \Rightarrow \Delta}{\Gamma_1, B, A, \Gamma_2 \Rightarrow \Delta} \qquad (RP)\quad \frac{\Gamma \Rightarrow \Delta_1, A, B, \Delta_{,2}}{\Gamma \Rightarrow \Delta_1, B, A, \Delta_2}$$

$$(LC)\quad \frac{A, A, \Gamma \Rightarrow \Delta}{A, \Gamma \Rightarrow \Delta} \qquad (RC)\quad \frac{\Gamma \Rightarrow \Delta, A, A}{\Gamma \Rightarrow \Delta, A}$$

Regra do corte: $$\frac{\Gamma_1 \Rightarrow \Delta_1, A \qquad A, \Gamma_2 \Rightarrow \Delta_2}{\Gamma_1, \Gamma_2 \Rightarrow \Delta_1, \Delta_2}$$

Restrição: nas regras $(L\exists)$ e $(R\forall)$, a variável y não ocorre livre em A, nem em alguma fórmula de Γ ou Δ

Uma *derivação* no sistema **CS** é um encadeamento de aplicações de regras de inferência em forma de árvore (figura de prova) cujos nós são seqüentes. Mais precisamente, se Π_1,...,Π_n, $0 \leq n \leq 2$, são derivações, s um seqüente e r uma aplicação de uma regra de inferência, então

$$\frac{\Pi_1, ...\Pi_n}{s}\, r$$

é uma derivação.

As regras de inferência são classificadas em dois grupos: regras de introdução à esquerda, $\{L\wedge, L\vee, L\rightarrow, L\sim, L\forall, L\exists, LW, LP, LC\}$, e regras de introdução à direita, $\{R\wedge, R\vee, R\rightarrow, R\sim, R\forall, R\exists, RW, RP, RC\}$. As regras lógicas de introdução à esquerda e à direita correspondem respectivamente às regras introdução e eliminação de um sistema em dedução natural e desempenham, de certa forma, o mesmo papel dessas regras. As regras estruturais, atenuação (LW) e (RW), permutação (LP) e (RP), e contração (LC) e (RC), são regras de inferência que não envolvem qualquer tipo de símbolo lógico.

Na regra do corte, a fórmula A é a fórmula cortada cuja complexidade determina o grau da aplicação desta regra em uma derivação. A complexidade de uma fórmula é o número de ocorrências de símbolos lógicos diferentes de $\perp$ nessa fórmula.

O *grau de uma derivação* Π é o grau máximo de uma aplicação da regra do corte nesta derivação. O *nível* de uma aplicação de um corte em uma derivação Π é determinado pelo número de seqüentes da subderivação de Π que termina com o corte considerado.

O sistema **CS** satisfaz o Teorema de eliminação do corte e tem como consequência importantes resultados tais como o Princípio de subfórmula e os Teoremas de consistência e interpolação. O Teorema de eliminação do corte garante que qualquer seqüente derivável neste sistema, através da regra do corte, pode ser igualmente derivável sem esta regra. A sua demonstração segue por indução dupla no grau de uma derivação Π e no nível do corte. Uma vez escolhida a aplicação do corte com grau máximo, esta aplicação é eliminada por indução no nível deste corte.

4. Lógica da Provabilidade

A idéia embrionária da Lógica da Provabilidade surgiu no famoso artigo de Gödel [5] em 1931, no qual, é apresentado uma formalização dos conceitos de cunho sintático-morfológico da Aritmética de Peano, **PA**, nela própria. Em particular, Gödel formalizou o conceito "ser demonstrável na aritmética de Peano", representado pelo predicado de primeira ordem Bew. Mais precisamente, $Bew(x)$ é uma abreviação da fórmula $\exists y Pf(y, x)$ da Aritmética de Peano, onde $Pf(y, x)$ é a fórmula que expressa a propriedade "y é o número de Gödel de uma prova da fórmula cujo número de Gödel é x".

O predicado Bew tem três propriedades, conhecidas como as condições de derivabilidade de Hilbert-Bernays-Löb, que desempenham um papel importante na Lógica da Provabilidade, a saber:
(i) se $\vdash_{PA} S$, então $\vdash_{PA} Bew(\ulcorner S \urcorner)$
(ii) $\vdash_{PA} Bew(\ulcorner R \rightarrow S \urcorner) \rightarrow (Bew(\ulcorner R \urcorner) \rightarrow Bew(\ulcorner S \urcorner))$
(iii) $\vdash_{PA} Bew(\ulcorner S \urcorner) \rightarrow Bew(\ulcorner Bew(\ulcorner S \urcorner) \urcorner)$

onde R e S são sentenças da Aritmética de Peano e $\ulcorner e \urcorner$ representa o número de Gödel de uma expressão e.

A primeira condição nos diz que se uma sentença S é demonstrável, então também o é a sentença que expressa que S é demonstrável. De acordo com a segunda condição, é sempre demonstrável em **PA** que se um condicional e seu antecedente são demonstráveis, então o conseqüente também o é. A terceira é uma formalização em **PA** da primeira condição.

A Lógica da Provabilidade, denominada **GL**, em homenagem a Gödel e Löb, é uma lógica proposicional modal na qual os operadores modais de necessidade e possibilidade, representados pelos símbolos $\Box$ e $\Diamond$ respectivamente, ganham um novo significado. Em **GL**, o operador modal $\Box$ é interpretado como "ser demonstrável na aritmética de Peano", enquanto que operador $\Diamond$ significa "ser consistente com a aritmética de Peano".

A linguagem de **GL** é constituída pelo conjunto $\{\rightarrow, \wedge, \vee, \sim, \Box\}$ de símbolos lógicos, além dos usuais símbolos não lógicos.
Símbolo definido: $\Diamond A =_{def} (\sim \Box \sim A)$

Os postulados de GL são:

(1) Todas as tautologias são axiomas
(2) $\Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B)$
(4) $\Box(\Box A \rightarrow A) \rightarrow \Box A$
(5) se $\vdash_{GL} A$ e $\vdash_{GL} A \rightarrow B$, então $\vdash_{GL} B$
(6) se $\vdash_{GL} A$, então $\vdash_{GL} \Box A$.

Qual a relação entre o predicado de primeira ordem *Bew* da Aritmética de Peano e o operador modal $\Box$ de GL? Robert Solovay [8] tratou esta questão de forma rigorosa e precisa. Ele interpretou a lógica **GL** na Aritmética de Peano através de uma função tradução * e mostrou que uma fórmula A é teorema de **GL** se e somente se, A^* é teorema de **PA**. Isto significa que o predicado *Bew* na Aritmética de Peano comporta-se como um operador modal.

Do ponto de vista semântico, **GL** é correta e completa com respeito à classe de modelos de Kripke cujas relações de acessibilidade são transitivas e têm inversas bem-fundadas. Lembramos que um modelo de Kripke é uma tripla $< W, R, V >$, constituída de um domínio W (conjunto dos mundos possíveis), uma relação R sobre W (relação de acessibilidade) e uma função V que associa mundos à variáveis proposicionais de uma dada linguagem, especificando que variável proposicional é verdadeira em que mundo.

Agradeço aos professores José Eduardo de Almeida Moura e Luiz Carlos Pereira pela leitura atenciosa e sugestões.

Referências

1. BUSS S. R. (ed.) *Handbook of Proof Theory.* Amsterdam: Elsevier, 1998
2. BOOLOS, G. *The Logic of Provability.* Cambridge: Cambridge University, 1993.
3. GIRARD, J.Y. *Proof Theory and Logical Complexity.* Napoli: Bibliopolis, 1987.
4. GENTZEN, G. Investigations into Logical Deduction. In - SZABO, M. E. *The Collected paper of Gerhard Gentzen.* Amsterdam: North-Holland, 1969.

5. GÖDEL, K. On formally undecidable propositions of Principia Mathematica and related systems I. In - FEFERMAN, S. et al., (eds.) *Collected Works*, vol I. New York: Claredon, 1986(a), p. 287 - 295.
6. PEREIRA, L. C. e MASSI, C. D. B. Normalização para a lógica clássica. *O que nos faz pensar: Cadernos do Departamento de Filosofia da PUC-Rio*, n. 2, p. 49-53, 1990.
7. PRAWITZ, D. *Natural Deduction*, Almqvist & Wiksel, Stockholm, 1965
8. SOLOVAY, R. M. Provability Interpretatios of Modal Logic. *Israel Journal of Mathematics* 25,1976, pp 287-304.
9. TROELSTRA, A. S. SCHWICHTENBERG, H. *Basic Proof Theory.* vol I, Amsterdam: North-Holland, 1980.

UFRN - Departamento de filosopia, 59072-970, Natal, RN, Brasil
E-mail address: mpaz@ufrnet.br