Uma formalização da interpretação modal do sistema intuicionista

Elian Babireski

2024

Sumário

"Oh, you can't help that," said the Cat: "we're all mad here. I'm mad. You're mad." "How do you know I'm mad?" said Alice. "You must be," said the Cat, "or you wouldn't have come here."

—Lewis Carroll, *Alice in Wonderland*

Capítulo 1

Introdução

As lógicas modais consistem em um conjunto de extensões da lógica clássica que contam com a adição de um ou mais operadores, chamados modalidades, que qualificam sentenças. No caso do sistema **S4**, são adicionadas as modalidades de necessidade ($\Box$) e possibilidade ($\Diamond$) em conjunto à regra da necessitação[1] e os axiomas **K**: $\Box(A \rightarrow B) \rightarrow \Box A \rightarrow \Box B$, **T**: $\Box A \rightarrow A$ e **4**: $\Box A \rightarrow \Box\Box A$ [7]. Ademais, pode-se derivar nesse sistema, por meio da dualidade entre as modalidades[2], sentenças duais aos axiomas **T** e **4**, sendo elas $\mathbf{T}_\Diamond$: $A \rightarrow \Diamond A$ e $\mathbf{4}_\Diamond$: $\Diamond\Diamond A \rightarrow \Diamond A$, respectivamente [**?**].

As mônadas ganharam destaque na área de linguagens de programação desde que [5] formalizou uma metalinguagem que faz uso dessas estruturas para modelar noções de computação – como parcialidade, não-determinismo, exceções e continuações – de uma maneira puramente funcional. Pode-se notar uma grande semelhança entre as sentenças $\mathbf{T}_\Diamond$ e $\mathbf{4}_\Diamond$ e as transformações naturais monádicas η: $1_C \rightarrow T$ e μ: $T^2 \rightarrow T$, respectivamente. Nesse sentido, [6] demonstraram que se pode traduzir essa metalinguagem para o sistema **S4** da lógica modal, pelo qual se torna interessante analisar esse sistema como uma linguagem de programação sob a ótica do isomorfismo de Curry-Howard.

[7] apresentam duas traduções equivalentes da lógica intuicionista para o sistema **S4** da lógica modal, sendo um deles correspondente a uma abordagem *call-by-name* e outra a um abordagem *call-by-value*. Tais traduções possuem grande similaridade com as traduções da lógica intuicionista para a lógica linear definidas por [2]. Essas traduções equivalem à tradução por negação dupla que, por sua vez, equivalem a traduções *continuation-passing style* (CPS) em compiladores por meio do isomorfismo de Curry-Howard [**?**], o que torna esse tema interessante no ponto de vista de compilação.

Durante grande parte da história, provas lógicas e matemáticas eram validadas manualmente pela comunidade acadêmica, o que muitas vezes – a depender do tamanho e complexidade da prova – se mostrava ser um trabalho

[1] Se $\vdash A$ então $\vdash \Box A$

[2] $\Diamond A \equiv \neg\Box\neg A$

complexo e sujeito a erros. Hoje em dia, exitem *softwares* chamados assistentes de provas que permitem verificar – graças ao isomorfismo de Curry-Howard – a corretude de provas [**?**]. O assistente de provas que será usado neste trabalho é o Coq, que utiliza o cálculo de construções indutivas e um conjunto axiomático pequeno para permitir a escrita de provas simples e intuitivas [**?**].

Este trabalho será uma continuação do desenvolvimento da biblioteca de lógica modal no assistente de provas Coq feito em [**?**] e posteriormente expandido de forma a permitir a fusão de lógicas modais em [**?**]. Uma formalização similar de traduções de lógicas foi feito em [**?**], porém, neste caso, das lógicas clássica e intuicionista para a lógica linear.

1.1 Justificativa

1.2 Intenções

1.3 Estruturação

Capítulo 2

Fundamentação

2.1 Sistema

Para este trabalho, a definição de sistema adotada será uma especialização daquela provida por Béziau [1].

Definição 1 (Sistema). *Um sistema consiste num par* $\mathbf{L} = \langle \mathcal{L}, \vdash \rangle$*, onde* $\mathcal{L}$ *consiste em um conjunto de sentenças bem-formadas e* $\vdash : \wp(\mathcal{L}) \times \mathcal{L}$ *em uma relação de dedução, sem demais condições.* □

Definiremos a noção de profundidade de uma sentença para que possamos realizar indução na profundidade da sentença, conforme Troelstra [7].

Definição 2 (Profundidade). *A profundidade* $|\alpha|$ *de uma sentença* α *consiste no comprimento do maior ramo de sua árvore de construção. Seja* $\circ$ *um operador qualquer, define-se a profundidade recursivamente como:*

$$
\begin{aligned}
|p| &:= 0 \\
|\bot| &:= 0 \\
|\circ\,\alpha| &:= |\alpha| + 1 \\
|\alpha \circ \beta| &:= \max(|\alpha|, |\beta|) + 1
\end{aligned}
$$ □

Definição 3 (Substituição). *Uma substituição consiste em uma função* $\sigma : \mathcal{P} \to \mathcal{L}$ *que mapeia proposições em sentenças. A aplicação de* σ *em uma sentença* $\varphi \in \mathcal{L}$*, denotada* $\varphi[\sigma]$*, define-se recursivamente como a aplicação de* σ *a cada proposição* $p \in \mathcal{P}$ *em* φ*.*

$$
\begin{aligned}
p[p \mapsto \beta] &:= \beta \\
q[p \mapsto \beta] &:= q \\
\bot[p \mapsto \beta] &:= \bot \\
\circ\alpha[p \mapsto \beta] &:= \circ(\alpha[p \mapsto \beta]) \\
\alpha \circ \beta[p \mapsto \beta] &:= (\alpha[p \mapsto \beta]) \circ (\beta[p \mapsto \beta])
\end{aligned}
$$ □

Definição 4 ($\mathcal{L}_\mathbf{I}$)**.** *Define-se a linguagem do sistema intuicionista, denotada $\mathcal{L}_\mathbf{I}$, como o menor conjunto induzido a partir das seguintes regras:*

Definição 5 ($\vdash_\mathbf{I}$)**.** *Define-se a relação de dedução do sistema intuicionista, denotado $\vdash_\mathbf{I}$.*

Definição 6 ($\mathcal{L}_\mathbf{M}$)**.** *Define-se a linguagem dos sistemas modais, denotada $\mathcal{L}_\mathbf{M}$, como o menor conjunto induzido a partir das seguintes regras:*

$\top, \bot \in \mathcal{L}_\mathbf{I}$
$\mathcal{P} \subseteq \mathcal{L}_\mathbf{I}$
$\varphi \in \mathcal{L}_\mathbf{I} \Rightarrow \circ\varphi \in \mathcal{L}_\mathbf{I}$*, para* $\circ \in \{\Box, \Diamond, \neg\}$
$\varphi, \psi \in \mathcal{L}_\mathbf{I} \Rightarrow \varphi \circ \psi \in \mathcal{L}_\mathbf{I}$*, para* $\circ \in \{\wedge, \vee, \rightarrow\}$

Definição 7 (Dedução)**.** *Uma dedução para uma linguagem $\mathcal{L}$ consiste em um par composto por um conjunto finito $\{\varphi_1, \cdots, \varphi_n\} \subseteq \mathcal{L}$, chamado de* premissas*, e uma sentença $\varphi \in \mathcal{L}$, chamada de* conclusão*, que pode ser notada da seguinte forma:*

$$\frac{\varphi_1 \cdots \varphi_n}{\varphi} \ .$$

Definição 8 (Sistema de Hilbert)**.** *Um sistema de Hilbert para um sistema $\mathbf{L} = \langle \mathcal{L}, \vdash \rangle$ consiste em um par $\mathcal{H} = \langle \mathcal{A}, \mathcal{R} \rangle$, sendo $\mathcal{A}$ um conjunto de axiomas e $\mathcal{R}$ um conjunto de regras de dedução. Uma sucessão $(\varphi_i)_{i=1}^n$, onde cada sentença φ_i trata-se de um axioma $\alpha \in \mathcal{A}$, uma assunção $\gamma \in \Gamma$ ou sentenças geradas pela aplicação de regras de dedução $\rho \in \mathcal{R}$ a sentenças anteriores, consiste em uma prova de $\Gamma \vdash \varphi_n$.*

2.2 Tradução

Traduções entre sistemas consistem em funções que mapeiam sentenças de um sistema a sentenças de outro sistema e garantem certas propriedades. As propriedades a serem garantidas variam e ainda são discutidas na literatura, deixando a definição exata de tradução – assim como houve com a definição de sistema – varie de acordo com a predileção de cada autor. Nesta seção, serão abordadas historicamente noções de tradução entre sistemas, bem como serão definidos e nomeados os conceitos de tradução que serão usados no restante deste trabalho.

Definição 9 (Tradução)**.** *Uma sentença φ de um sistema $\mathbf{A} = \langle \mathcal{L}_\mathbf{A}, \vdash_\mathbf{A} \rangle$ pode ser traduzida a uma sentença φ^* em um sistema $\mathbf{B} = \langle \mathcal{L}_\mathbf{B}, \vdash_\mathbf{B} \rangle$ caso exista uma função $\bullet^* : \mathcal{L}_\mathbf{A} \rightarrow \mathcal{L}_\mathbf{B}$ que garanta que $\Gamma \vdash_\mathbf{A} \varphi \Leftrightarrow \Gamma^* \vdash_\mathbf{B} \varphi^*$.* □

Definição 10 ($\bullet^\neg$)**.** *Define-se a tradução $\bullet^\neg$ indutivamente da seguinte maneira:*

$$\begin{aligned} p^\neg &:= \neg\neg p \\ \bot^\neg &:= \bot \\ (\varphi \wedge \psi)^\neg &:= \neg\neg(\varphi^\neg \wedge \psi^\neg) \\ (\varphi \vee \psi)^\neg &:= \neg\neg(\varphi^\neg \vee \psi^\neg) \\ (\varphi \rightarrow \psi)^\neg &:= \neg\neg(\varphi^\neg \rightarrow \psi^\neg) \end{aligned}$$ □

A primeira tradução do sistema intuicionista ao sistema modal foi proposta por Gödel [3] motivado pela possibilidade de leitura da necessidade como uma modalidade de construtividade. Ou seja, por meio dessa tradução, a sentença $\Box\varphi$ poderia ser lida como φ *pode ser provada construtivamente* [7]. Gödel conjeiturou a corretude fraca dessa tradução, que foi posteriormente provada por McKinsey e Tarski [4] em conjunto com sua completude fraca.

Definição 11 ($\bullet^\circ$). *Define-se a tradução $\bullet^\circ$ indutivamente da seguinte maneira:*

$$\begin{aligned} p^\circ &:= p \\ \bot^\circ &:= \bot \\ (\varphi \wedge \psi)^\circ &:= \varphi^\circ \wedge \psi^\circ \\ (\varphi \vee \psi)^\circ &:= \Box\varphi^\circ \vee \Box\psi^\circ \\ (\varphi \to \psi)^\circ &:= \Box\varphi^\circ \to \psi^\circ \end{aligned}$$

□

Definição 12 ($\bullet^\Box$). *Define-se a tradução $\bullet^\Box$ indutivamente da seguinte maneira:*

$$\begin{aligned} p^\Box &:= \Box p \\ \bot^\Box &:= \bot \\ (\varphi \wedge \psi)^\Box &:= \varphi^\Box \wedge \psi^\Box \\ (\varphi \vee \psi)^\Box &:= \varphi^\Box \vee \psi^\Box \\ (\varphi \to \psi)^\Box &:= \Box(\varphi^\Box \to \psi^\Box) \end{aligned}$$

□

Faz-se interessante pontuar que as traduções $\bullet^\circ$ e $\bullet^\Box$ correspondem, respectivamente, às traduções $\bullet^\circ$ e $\bullet^*$ do sistema intuicionista ao sistema linear providas por Girard [2], sendo as primeiras correspondentes a uma ordem de avaliação por nome (*call-by-name*) e as segundas a uma ordem de avaliação por valor (*call-by-value*).

Lema 1. $\forall\alpha \in \mathcal{L}_\mathbf{I}.\, \Box\alpha^\circ \leftrightarrow \alpha^\Box$.

Demonstração. Prova por indução na profundidade de α. □

Lema 2. $\forall\alpha \in \mathcal{L}_\mathbf{I}.\, \Box\alpha^\Box \leftrightarrow \alpha^\Box$.

Demonstração. A volta $\Box\alpha^\Box \leftarrow \alpha^\Box$ pode ser provada trivialmente por meio da regra da necessitação. A ida $\Box\alpha^\Box \to \alpha^\Box$ deve ser provada por indução na profundidade de α. □

Teorema 1. $\Gamma \vdash_\mathbf{M} \alpha \to \beta \Leftrightarrow \Gamma \cup \{\alpha\} \vdash_\mathbf{M} \beta$.

Demonstração. Prova por indução no tamanho da prova. □

Teorema 2. $\forall\alpha \in \mathcal{L}_\mathbf{I}.\Gamma \vdash_\mathbf{I} \alpha \Rightarrow \Gamma^\Box \vdash_\mathbf{M} \alpha^\Box$

Demonstração. Sabe-se que $\Gamma \vdash_\mathbf{I} \alpha$, portanto existe uma prova $\mathcal{P} = \mathcal{P} + (\alpha)$, onde $\mathcal{P}$ consiste em uma sucessão finita e possivelmente vazia.

Caso. $\mathcal{P} = (\alpha)$.

Existem dois casos para uma prova $\mathcal{P}$ de tamanho $|\mathcal{P}| = 1$.

Caso. $\alpha \in \mathcal{A}$.

Prova.

Caso. $\alpha \in \Gamma$.

Prova.

□

Definição 13 (Sucessão)**.** *Uma sucessão consiste em uma coleção ordenada de elementos que permite repetição.*

Definição 14 (Concatenação)**.** *Uma sucessão consiste em uma coleção de elementos*

Capítulo 3

Formalização

Capítulo 4

Implementação

Capítulo 5

Conclusão

Referências Bibliográficas

[1] Jean-Yves Béziau. Universal logic. *Logica*, 1994.

[2] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 1987.

[3] Kurt Gödel. Eine Interpretation des intuitionistischen Aussagenkalküls. *Ergebnisse eines Mathematischen Kolloquiums*, 1933.

[4] John Charles Chenoweth McKinsey and Alfred Tarski. Some theorems about the sentential calculi of Lewis and Heyting. *The Journal of Symbolic Logic*, 1948.

[5] Eugenio Moggi. Notions of computation and monads. *Information and Computation*, 1991.

[6] Frank Pfenning and Rowan Davies. A judgmental reconstruction of modal logic. *Mathematical Structures in Computer Science*, 2001.

[7] Anne Sjerp Troelstra and Helmut Schwichtenberg. *Basic proof theory*. Cambridge University Press, 2000.