Uma formalização da interpretação modal do sistema intuicionista

Elian Babireski

2024

Resumo

Resumo aqui.

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**: $\Box(A \to B) \to \Box A \to \Box B$, **T**: $\Box A \to A$ e **4**: $\Box A \to \Box\Box A$ [**?**]. Ademais, pode-se derivar nesse sistema, por meio da dualidade entre as modalidades[2], sentenças duais aos axiomas **T** e **4**, sendo elas $\mathbf{T}_\Diamond$: $A \to \Diamond A$ e $\mathbf{4}_\Diamond$: $\Diamond\Diamond A \to \Diamond A$, respectivamente [**?**].

As mônadas ganharam destaque na área de linguagens de programação desde que [**?**] 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 $\boldsymbol{\eta}$: $1_C \to T$ e $\boldsymbol{\mu}$: $T^2 \to T$, respectivamente. Nesse sentido, [**?**] 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.

[**?**] 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 [**?**]. 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 complexo e sujeito a erros. Hoje em dia, exitem *softwares* chamados assistentes de provas

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

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

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

Notação 1. *A marcação $\bullet$ consiste em um marcador de posição, ou seja, pode ser trocado por qualquer valor.*

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

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 [**?**].

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

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

Definição 3 (Esquema)**.** *Definição.*

Definição 4 ($\mathcal{L}_\mathbf{I}$)**.** *A linguagem do sistema intuicionista, denotada $\mathcal{L}_\mathbf{I}$, consiste no menor conjunto induzido a partir das seguintes regras:*

$$
\begin{aligned}
&\bot \in \mathcal{L}_\mathbf{I} \\
&\mathcal{P} \subseteq \mathcal{L}_\mathbf{I} \\
&\alpha, \beta \in \mathcal{L}_\mathbf{I} \Rightarrow \alpha \circ \beta \in \mathcal{L}_\mathbf{I},\ \textit{para}\ \circ \in \{\wedge, \vee, \to\}.
\end{aligned}
$$
□

Definição 5 ($\mathcal{L}_\mathbf{M}$). *A linguagem do sistemas modais, denotada $\mathcal{L}_\mathbf{M}$, consiste no menor conjunto induzido a partir das seguintes regras:*

$$\begin{aligned}
&\bot \in \mathcal{L}_\mathbf{M}\\
&\mathcal{P} \subseteq \mathcal{L}_\mathbf{M}\\
&\alpha \in \mathcal{L}_\mathbf{M} \Rightarrow \Box\,\alpha \in \mathcal{L}_\mathbf{M}\\
&\alpha, \beta \in \mathcal{L}_\mathbf{M} \Rightarrow \alpha \circ \beta \in \mathcal{L}_\mathbf{M},\ \textit{para}\ \circ \in \{\wedge, \vee, \rightarrow\}.
\end{aligned}$$ □

Definição 6 (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 7 (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 esquemas axiomas e $\mathcal{R}$ um conjunto de regras de dedução. Uma sucessão $\langle \varphi_i \mid 1 \leq i \leq n \rangle$, 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 8 (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 $\bullet^*\colon \mathcal{L}_\mathbf{A} \rightarrow \mathcal{L}_\mathbf{B}$ que garanta que $\Gamma \vdash_\mathbf{A} \varphi \Leftrightarrow \Gamma^* \vdash_\mathbf{B} \varphi^*$.* □

Definição 9 ($\bullet^\neg$). *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 [**?**] 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* [**?**]. Gödel conjeiturou a corretude fraca dessa tradução, que foi posteriormente provada por McKinsey e Tarski [**?**] em conjunto com sua completude fraca.

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

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

□

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

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

□

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 [**?**], 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. Como $\Gamma \vdash_{\mathbf{I}} \alpha$, sabe-se que existe uma prova $\langle \varphi_i \mid 1 \leq i \leq n \rangle$ tal que $\varphi_n = \alpha$. A demonstração deste teorema será feita por indução no tamanho n da prova.

Passo ($n = 1$)**.** A prova, caso possua tamanho $n = 1$, tem obrigatoriamente a forma $\langle \alpha \rangle$. Deste modo, existem duas casos a serem considerados: α ser um axioma ou α ser uma premissa.

> **Caso 1** ($\alpha \in \Gamma$)**.** Como $\alpha \in \Gamma$, sabe-se que $\alpha^{\Box} \in \Gamma^{\Box}$, uma vez que $\Gamma^{\Box} = \{\varphi^{\Box} \mid \varphi \in \Gamma\}$. Desta forma, $\langle \alpha^{\Box} \rangle$ constitui uma prova para $\Gamma^{\Box} \vdash \alpha^{\Box}$.

Caso 2 ($\alpha \in \mathcal{A}$).

Caso 2.1 ($\mathbf{A_1}$).

1	$\alpha^{\Box} \to \beta^{\Box} \to \alpha^{\Box}$	$\mathbf{A_1}$
2	$\Box(\alpha^{\Box} \to \beta^{\Box} \to \alpha^{\Box})$	$\mathbf{R_2}$ 1
3	$\Box(\alpha^{\Box} \to \beta^{\Box} \to \alpha^{\Box}) \to \Box\,\alpha^{\Box} \to \Box(\beta^{\Box} \to \alpha^{\Box})$	$\mathbf{A_{11}}$
4	$\Box\,\alpha^{\Box} \to \Box(\beta^{\Box} \to \alpha^{\Box})$	$\mathbf{R_1}$ 2 3
5	$\Box(\Box\,\alpha^{\Box} \to \Box(\beta^{\Box} \to \alpha^{\Box}))$	$\mathbf{R_2}$ 4

Caso 2.2 ($\mathbf{A_2}$).

Caso 2.3 ($\mathbf{A_3}$).

1	$\alpha^{\Box} \to \beta^{\Box} \to \alpha^{\Box} \wedge \beta^{\Box}$	$\mathbf{A_4}$
2	$\Box(\alpha^{\Box} \to \beta^{\Box} \to \alpha^{\Box} \wedge \beta^{\Box})$	$\mathbf{R_2}$ 1
3	$\Box(\alpha^{\Box} \to \beta^{\Box} \to \alpha^{\Box} \wedge \beta^{\Box}) \to \Box(\alpha^{\Box} \to \beta^{\Box}) \to \Box(\alpha^{\Box} \wedge \beta^{\Box})$	$\mathbf{A_{11}}$
4	$\Box(\alpha^{\Box} \to \beta^{\Box}) \to \Box(\alpha^{\Box} \wedge \beta^{\Box})$	$\mathbf{R_1}$ 2 3
5	$\Box(\Box(\alpha^{\Box} \to \beta^{\Box}) \to \Box(\alpha^{\Box} \wedge \beta^{\Box}))$	$\mathbf{R_2}$ 4

Caso 2.4 ($\mathbf{A_4}$).

1	$\alpha^{\Box} \wedge \beta^{\Box} \to \alpha^{\Box}$	$\mathbf{A_4}$
2	$\Box(\alpha^{\Box} \wedge \beta^{\Box} \to \alpha^{\Box})$	$\mathbf{R_2}$ 1

Caso 2.5 ($\mathbf{A_5}$).

1	$\alpha^{\Box} \wedge \beta^{\Box} \to \beta^{\Box}$	$\mathbf{A_5}$
2	$\Box(\alpha^{\Box} \wedge \beta^{\Box} \to \beta^{\Box})$	$\mathbf{R_2}$ 1

Caso 2.6 ($\mathbf{A_6}$).

1	$\alpha^{\Box} \to \alpha^{\Box} \vee \beta^{\Box}$	$\mathbf{A_7}$
2	$\Box(\alpha^{\Box} \to \alpha^{\Box} \vee \beta^{\Box})$	$\mathbf{R_2}$ 1

Caso 2.7 ($\mathbf{A_7}$).

1	$\beta^{\Box} \to \alpha^{\Box} \vee \beta^{\Box}$ [9]	$\mathbf{A_8}$
2	$\Box(\beta^{\Box} \to \alpha^{\Box} \vee \beta^{\Box})$	$\mathbf{R_2}$ 1

Caso 2.8 ($\mathbf{A_8}$).

$\square$

Definição 12. *A axiomatização do sistema intuicionista consiste nos seguintes esquemas e regras:*

$\mathbf{A_1}$	$\alpha \to \beta \to \alpha$
$\mathbf{A_2}$	$(\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to (\alpha \to \gamma)$
$\mathbf{A_3}$	$\alpha \to \beta \to \alpha \wedge \beta$
$\mathbf{A_4}$	$\alpha \wedge \beta \to \alpha$
$\mathbf{A_5}$	$\alpha \wedge \beta \to \beta$
$\mathbf{A_6}$	$\alpha \to \alpha \vee \beta$
$\mathbf{A_7}$	$\beta \to \alpha \vee \beta$
$\mathbf{A_8}$	$(\alpha \to \gamma) \to (\beta \to \gamma) \to (\alpha \vee \beta \to \gamma)$
$\mathbf{A_9}$	$\bot \to \alpha$
$\mathbf{R_1}$	*Se* $\vdash \alpha$ *e* $\vdash \alpha \to \beta$, *então* $\vdash \beta$.

$\square$

Definição 13. *A axiomatização do sistema modal consiste nos seguintes esquemas e regras:*

$\mathbf{A_1}$	$\alpha \to \beta \to \alpha$
$\mathbf{A_2}$	$(\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to (\alpha \to \gamma)$
$\mathbf{A_3}$	$(\neg\alpha \to \neg\beta) \to \alpha \to \beta$
$\mathbf{A_4}$	$\alpha \to \beta \to \alpha \wedge \beta$
$\mathbf{A_5}$	$\alpha \wedge \beta \to \alpha$
$\mathbf{A_6}$	$\alpha \wedge \beta \to \beta$
$\mathbf{A_7}$	$\alpha \to \alpha \vee \beta$
$\mathbf{A_8}$	$\beta \to \alpha \vee \beta$
$\mathbf{A_9}$	$(\alpha \to \gamma) \to (\beta \to \gamma) \to (\alpha \vee \beta \to \gamma)$
$\mathbf{A_{10}}$	$\neg\neg\alpha \to \alpha$
$\mathbf{A_{11}}$	$\Box(\alpha \to \beta) \to \Box\,\alpha \to \Box\,\beta$
$\mathbf{A_{12}}$	$\Box\,\alpha \to \alpha$
$\mathbf{A_{13}}$	$\Box\,\alpha \to \Box\,\Box\,\alpha$
$\mathbf{A_{14}}$	$\Diamond(\alpha \vee \beta) \to \Diamond\,\alpha \vee \Diamond\,\beta$
$\mathbf{R_1}$	*Se* $\vdash \alpha$ *e* $\vdash \alpha \to \beta$, *então* $\vdash \beta$
$\mathbf{R_2}$	*Se* $\vdash \alpha$, *então* $\vdash \Box\,\alpha$

$\square$

Definição 14 (Sucessão)**.** *Uma sucessão, denotada por* $\langle\bullet\rangle$, *consiste em uma coleção ordenada de elementos que permite repetição. A notação* $\langle a_n | 1 \leq n \leq k\rangle$ *denota uma sucessão iniciada em* a_1 *e terminada em* a_k.

Definição 15 (Concatenação)**.** *A concatenação de duas sucessões* $\mathbf{A}$ *e* $\mathbf{B}$*, denotada* $\mathbf{A} + \mathbf{B}$ *consiste em uma nova sucessão resultante da justaposição dos elementos de* $\mathbf{A}$ *sucedidos pelos elementos de* $\mathbf{B}$*, mantendo a ordem original de ambos.*

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.