

Uma formalização da interpretação modal do sistema intuicionista

Elían Babireski

2024

Resumo

Resumo aqui.

Sumário

| | | |
|----------|-------------------------|----------|
| 1 | Introdução | 3 |
| 1.1 | Justificativa | 4 |
| 1.2 | Metas | 4 |
| 1.3 | Estruturação | 4 |
| 2 | Fundamentação | 5 |
| 2.1 | Sistemas | 5 |
| 2.2 | Traduções | 6 |
| 2.3 | Provadores | 7 |
| 3 | Formalização | 8 |
| 3.1 | Sistemas | 8 |
| 3.2 | Traduções | 12 |
| 3.3 | Corretude | 14 |
| 3.4 | Compleitude | 17 |

«‘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 necessitação¹ e os axiomas **K**: $\Box(A \rightarrow B) \rightarrow \Box A \rightarrow \Box B$, **T**: $\Box A \rightarrow A$ e **4**: $\Box A \rightarrow \Box \Box A$ (Troelstra and Schwichtenberg, 2000). Ademais, pode-se derivar nesse sistema, por meio da dualidade entre as modalidades², sentenças duais aos axiomas **T** e **4**, sendo elas **T** $_{\Diamond}$: $A \rightarrow \Diamond A$ e **4** $_{\Diamond}$: $\Diamond \Diamond A \rightarrow \Diamond A$, respectivamente Zach (2024).

As mônadas ganharam destaque na área de linguagens de programação desde que Moggi (1991) formalizou uma metalinguagem que faz uso dessas estruturas para modelar noções de computação — como parcialidade, não-determinismo, exceções e continuacões — de uma maneira puramente funcional. Pode-se notar uma grande semelhança entre as sentenças **T** $_{\Diamond}$ e **4** $_{\Diamond}$ e as transformações naturais monádicas η : $1_C \rightarrow T$ e μ : $T^2 \rightarrow T$, respectivamente. Nesse sentido, Pfenning and Davies (2001) 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.

Troelstra and Schwichtenberg (2000) 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 Girard (1987). 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

¹Se $\vdash A$ então $\vdash \Box A$

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

do tamanho e complexidade da prova — se mostrava ser um trabalho complexo e sujeito a erros. Hoje em dia, existem *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 Metas

1.3 Estruturação

Capítulo 2

Fundamentação

2.1 Sistemas

Conforme visto, as noções de sistema variam entre diferentes autores e permanece um campo em aberto. Para as necessidades deste trabalho, usaremos a definição proposta por Béziau (1994), uma vez que se trata de uma definição simples e que, portanto, não traz elementos irrelevantes aos intuítos deste trabalho.

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 sobre as sentenças, sem demais condições.* \square

Cabe destacar que a definição de sistema provida foi definida com base em \Vdash , uma relação qualquer entre as sentenças, que pode ser uma relação de dedução, denotada \vdash , ou uma relação de satisfação, denotada \models . Propriedades da tradução podem ser provadas sobre qualquer uma dessas relações, como veremos adiante. Entretanto, neste trabalho, serão abordadas somente as relações de dedução.

Definição 2 (Assinatura). *Uma assinatura consiste num conjunto de operadores e suas respectivas aridades. A notação \circ^n denota um operador \circ com aridade $n \in \mathbb{N}$.* \square

Definiremos a noção de profundidade de uma sentença para que possamos realizar indução na profundidade da sentença, conforme Troelstra and Schwichtenberg (2000).

Definição 3 (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:

$$\begin{aligned} |p| &:= 0 \\ |\perp| &:= 0 \\ |\circ \alpha| &:= |\alpha| + 1 \\ |\alpha \circ \beta| &:= \max(|\alpha|, |\beta|) + 1. \end{aligned} \quad \square$$

Definição 4 (Esquema). *Um esquema consiste em um padrão com metavariáveis que permitem representar um conjunto, geralmente infinito, de sentenças.* \square

Definição 5 (Regra). *Uma regra de dedução consiste num par $\langle \Gamma, \alpha \rangle$, sendo Γ um conjunto de sentenças chamadas de premissas e α uma sentença chamada conclusão.* \square

Definição 6 (Axiomatização). *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.* \square

Definição 7 (Dedução). *Uma dedução de $\Gamma \vdash \alpha$ consiste numa sucessão $\langle \varphi_i \mid 1 \leq i \leq n \rangle$ onde $\varphi_n = \alpha$ cada sentença φ_i trata-se de um axioma, uma premissa, ou a conclusão da aplicação de uma regra de dedução a sentenças anteriores.* \square

2.2 Traduções

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 $\bullet^* : \mathcal{L}_{\mathbf{A}} \rightarrow \mathcal{L}_{\mathbf{B}}$ que garanta que $\Gamma \vdash_{\mathbf{A}} \varphi \Leftrightarrow \Gamma^* \vdash_{\mathbf{B}} \varphi^*$.* \square

Notação. *Seja $\Gamma \in \wp(\mathcal{L}_{\mathbf{A}})$ um conjunto de sentenças e $\bullet^* : \mathcal{L}_{\mathbf{A}} \rightarrow \mathcal{L}_{\mathbf{B}}$ uma tradução. Γ^* denota o conjunto $\{\alpha^* \mid \alpha \in \mathcal{L}_{\mathbf{A}}\} \in \wp(\mathcal{L}_{\mathbf{B}})$, ou seja, a aplicação da tradução a todos os elementos do conjunto.* \square

Definição 9 (\bullet^\neg). *Define-se a tradução \bullet^\neg indutivamente da seguinte maneira:*

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

2.3 Provedores

Capítulo 3

Formalização

3.1 Sistemas

Definição 10 (\mathcal{L}_I). *A linguagem do sistema intuicionista, denotada \mathcal{L}_I , consiste no menor conjunto induzido a partir das seguintes regras:*

$$\begin{aligned} \perp &\in \mathcal{L}_I \\ \mathcal{P} &\subseteq \mathcal{L}_I \\ \alpha, \beta \in \mathcal{L}_I &\Rightarrow \alpha \circ \beta \in \mathcal{L}_I, \text{ para } \circ \in \{\wedge, \vee, \rightarrow\}. \end{aligned} \quad \square$$

Notação. *Serão usadas as seguintes abreviações:*

$$\begin{aligned} \top &:= \perp \rightarrow \perp \\ \neg \alpha &:= \alpha \rightarrow \perp \\ \alpha \leftrightarrow \beta &:= (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha) \end{aligned}$$

Definição 11. *A axiomatização do sistema intuicionista consiste nos seguintes esquemas e regras:*

$$\begin{aligned} \mathbf{A}_1 \quad &\alpha \rightarrow \beta \rightarrow \alpha \\ \mathbf{A}_2 \quad &(\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma) \\ \mathbf{A}_3 \quad &\alpha \rightarrow \beta \rightarrow \alpha \wedge \beta \\ \mathbf{A}_4 \quad &\alpha \wedge \beta \rightarrow \alpha \\ \mathbf{A}_5 \quad &\alpha \wedge \beta \rightarrow \beta \\ \mathbf{A}_6 \quad &\alpha \rightarrow \alpha \vee \beta \\ \mathbf{A}_7 \quad &\beta \rightarrow \alpha \vee \beta \\ \mathbf{A}_8 \quad &(\alpha \rightarrow \gamma) \rightarrow (\beta \rightarrow \gamma) \rightarrow (\alpha \vee \beta \rightarrow \gamma) \\ \mathbf{A}_\perp \quad &\perp \rightarrow \alpha \\ \mathbf{R}_1 \quad &\text{Se } \vdash \alpha \text{ e } \vdash \alpha \rightarrow \beta, \text{ então } \vdash \beta. \end{aligned} \quad \square$$

BABIRESKI: Blackburn et al. (2001) traz uma visão da evolução dos sistemas modais.

Definição 12 (\mathcal{L}_M). A linguagem dos sistemas modais, denotada \mathcal{L}_M , consiste no menor conjunto induzido a partir das seguintes regras:

$$\begin{aligned} \perp &\in \mathcal{L}_M \\ \mathcal{P} &\subseteq \mathcal{L}_M \\ \alpha \in \mathcal{L}_M &\Rightarrow \Box \alpha \in \mathcal{L}_M \\ \alpha, \beta \in \mathcal{L}_M &\Rightarrow \alpha \circ \beta \in \mathcal{L}_M, \text{ para } \circ \in \{\wedge, \vee, \rightarrow\}. \end{aligned} \quad \square$$

Notação. Serão usadas as seguintes abreviações:

$$\begin{aligned} \top &:= \perp \rightarrow \perp \\ \neg \alpha &:= \alpha \rightarrow \perp \\ \Diamond \alpha &:= \neg \Box \neg \alpha \\ \alpha \multimap \beta &:= \Box(\alpha \rightarrow \beta) \\ \alpha \leftrightarrow \beta &:= (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha) \end{aligned}$$

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

$$\begin{aligned} \mathbf{A}_1 & \quad \alpha \rightarrow \beta \rightarrow \alpha \\ \mathbf{A}_2 & \quad (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma) \\ \mathbf{A}_3 & \quad \alpha \rightarrow \beta \rightarrow \alpha \wedge \beta \\ \mathbf{A}_4 & \quad \alpha \wedge \beta \rightarrow \alpha \\ \mathbf{A}_5 & \quad \alpha \wedge \beta \rightarrow \beta \\ \mathbf{A}_6 & \quad \alpha \rightarrow \alpha \vee \beta \\ \mathbf{A}_7 & \quad \beta \rightarrow \alpha \vee \beta \\ \mathbf{A}_8 & \quad (\alpha \rightarrow \gamma) \rightarrow (\beta \rightarrow \gamma) \rightarrow (\alpha \vee \beta \rightarrow \gamma) \\ \mathbf{A}_{\neg} & \quad \neg \neg \alpha \rightarrow \alpha \\ \mathbf{B}_1 & \quad \Box(\alpha \rightarrow \beta) \rightarrow \Box \alpha \rightarrow \Box \beta \\ \mathbf{B}_2 & \quad \Box \alpha \rightarrow \alpha \\ \mathbf{B}_3 & \quad \Box \alpha \rightarrow \Box \Box \alpha \\ \mathbf{R}_1 & \quad \text{Se } \vdash \alpha \text{ e } \vdash \alpha \rightarrow \beta, \text{ então } \vdash \beta \\ \mathbf{R}_2 & \quad \text{Se } \vdash \alpha, \text{ então } \vdash \Box \alpha. \end{aligned} \quad \square$$

BABIRESKI: Ver Zach (2024) acerca dos axiomas duais e suas derivações.

Teorema 1. A partir dos axiomas modais \mathbf{B}_1 , \mathbf{B}_2 e \mathbf{B}_3 , podem-se derivar os seguintes axiomas duais:

$$\begin{aligned} \mathbf{B}_1^\diamond &:= \Box(\alpha \rightarrow \beta) \rightarrow \Diamond \alpha \rightarrow \Diamond \beta \\ \mathbf{B}_2^\diamond &:= \alpha \rightarrow \Diamond \alpha \\ \mathbf{B}_3^\diamond &:= \Diamond \Diamond \alpha \rightarrow \Diamond \alpha. \end{aligned}$$

Teorema 2. $\vdash \Box(\alpha \rightarrow \beta) \rightarrow \Diamond\alpha \rightarrow \Diamond\beta$.

Demonstração. Pode ser provado pela seguinte sucessão de dedução:

$$\begin{array}{l|l} 1 & (\Box\neg\alpha \rightarrow \neg\alpha) \rightarrow \neg\neg\alpha \rightarrow \neg\Box\neg\alpha \\ 2 & \Box\neg\alpha \rightarrow \neg\alpha \\ 3 & \neg\neg\alpha \rightarrow \neg\Box\neg\alpha \end{array}$$

□

Teorema 3. $\vdash \alpha \rightarrow \Diamond\alpha$.

Demonstração. Pode ser provado pela seguinte sucessão de dedução:

$$\begin{array}{l|l} 1 & (\Box\neg\alpha \rightarrow \neg\alpha) \rightarrow \neg\neg\alpha \rightarrow \neg\Box\neg\alpha \\ 2 & \Box\neg\alpha \rightarrow \neg\alpha \\ 3 & \neg\neg\alpha \rightarrow \neg\Box\neg\alpha \end{array}$$

□

Teorema 4. $\vdash \Diamond\Diamond\alpha \rightarrow \Diamond\alpha$.

Demonstração. Isso equivale, por reescrita, a demonstrar $\vdash \neg\Box\neg\neg\Box\neg\alpha \rightarrow \neg\Box\neg\alpha$, o que pode ser feito pela seguinte sucessão de dedução:

$$\begin{array}{l|l} 1 & (\Box\neg\alpha \rightarrow \neg\alpha) \rightarrow \neg\neg\alpha \rightarrow \neg\Box\neg\alpha \\ 2 & \Box\neg\alpha \rightarrow \neg\alpha \\ 3 & \neg\neg\alpha \rightarrow \neg\Box\neg\alpha \end{array}$$

□

Provaremos, para o sistema modal apresentado, uma variação do teorema da dedução baseado na implicação estrita, conforme proposto por Marcus (1953) de modo a permitir simplificar muitas das demonstrações apresentadas futuramente neste trabalho. **BABIRESKI:** Hakli and Negri (2012) apresentam uma discussão sobre a validade do metateorema da dedução e suas variantes nos sistemas modais. Quem sabe valha a pena escrever um pouco sobre isso, pois se trata de uma leitura interessante.

Teorema 5. $\forall \Gamma \cup \{\alpha, \beta\} \in \wp(\mathcal{L}_{\mathbf{M}}) . \Gamma \cup \{\alpha\} \vdash \beta \Rightarrow \Gamma \vdash \Box(\alpha \rightarrow \beta)$.

Demonstração. Seja Γ um conjunto de sentenças e sejam α e β sentenças de modo que $\Gamma \cup \{\alpha\} \vdash \beta$, deve-se provar que $\Gamma \vdash \Box(\alpha \rightarrow \beta)$. Como $\Gamma \cup \{\alpha\} \vdash \beta$, existe uma prova de β a partir de $\Gamma \cup \{\alpha\}$. A prova baseia-se numa indução sobre o tamanho n da prova.

Caso 1 (Base). Para a base requer-se considerar os seguintes casos: **(1)** β consiste num axioma, **(2)** $\beta \in \Gamma$ e **(3)** $\beta = \alpha$.

Caso 1.1 ($\beta \in \mathcal{A}$).

| | | |
|---|--|-------------------------------------|
| 1 | $\beta \rightarrow \alpha \rightarrow \beta$ | $\mathbf{A_1}$ |
| 2 | β | $\mathbf{A_\beta}$ |
| 3 | $\alpha \rightarrow \beta$ | $\mathbf{R_1} \langle 1, 2 \rangle$ |
| 4 | $\Box(\alpha \rightarrow \beta)$ | $\mathbf{R_2} \langle 3 \rangle$ |

Caso 1.2 ($\beta \in \Gamma$).

| | | |
|---|--|-------------------------------------|
| 1 | $\beta \rightarrow \alpha \rightarrow \beta$ | $\mathbf{A_1}$ |
| 2 | β | \mathbf{P} |
| 3 | $\alpha \rightarrow \beta$ | $\mathbf{R_1} \langle 1, 2 \rangle$ |
| 4 | $\Box(\alpha \rightarrow \beta)$ | $\mathbf{R_2} \langle 3 \rangle$ |

Caso 1.3 ($\beta = \alpha$).

| | | |
|---|-----------------------------------|----------------------------------|
| 1 | $\alpha \rightarrow \alpha$ | $\mathbf{L_1}$ |
| 2 | $\Box(\alpha \rightarrow \alpha)$ | $\mathbf{R_2} \langle 1 \rangle$ |

Caso 2 (Passo). Supõe-se que, para qualquer prova de $\Gamma \cup \{\alpha\} \vdash \beta$ com tamanho k , tem-se que $\Gamma \vdash \Box(\alpha \rightarrow \beta)$. Deve-se mostrar que a proposição segue verdadeira caso a prova tenha tamanho $k + 1$. Assim, sendo $\langle \varphi_i \mid 1 \leq i \leq k + 1 \rangle$ uma sucessão de dedução com $\varphi_{k+1} = \beta$, requer-se considerar os seguintes casos:

Caso 2.1 ($\beta \in \mathcal{A}$). *Vide* caso $\mathbf{C_{1.1}}$.

Caso 2.2 ($\beta \in \Gamma$). *Vide* caso $\mathbf{C_{1.2}}$.

Caso 2.3 ($\beta = \alpha$). *Vide* caso $\mathbf{C_{1.3}}$.

Caso 2.4 ($\mathbf{R_1}$). **BABIRESKI:** Aqui basta transcrever a prova da aula.

Caso 2.5 ($\mathbf{R_2}$). **BABIRESKI:** Estou sofrendo nesse caso.

□

3.2 Traduções

A primeira tradução do sistema intuicionista ao sistema modal foi proposta por Gödel (1933) 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* (Troelstra and Schwichtenberg, 2000). Gödel conjecturou a corretude fraca dessa tradução, que foi posteriormente provada por McKinsey and Tarski (1948) em conjunto com sua completude fraca.

Definição 14 (\bullet°). *Define-se a tradução \bullet° indutivamente da seguinte maneira:*

$$\begin{aligned} p^\circ &:= p \\ \perp^\circ &:= \perp \\ (\varphi \wedge \psi)^\circ &:= \varphi^\circ \wedge \psi^\circ \\ (\varphi \vee \psi)^\circ &:= \Box\varphi^\circ \vee \Box\psi^\circ \\ (\varphi \rightarrow \psi)^\circ &:= \Box\varphi^\circ \rightarrow \psi^\circ \end{aligned} \quad \square$$

Definição 15 (\bullet^\Box). *Define-se a tradução \bullet^\Box indutivamente da seguinte maneira:*

$$\begin{aligned} p^\Box &:= \Box p \\ \perp^\Box &:= \perp \\ (\varphi \wedge \psi)^\Box &:= \varphi^\Box \wedge \psi^\Box \\ (\varphi \vee \psi)^\Box &:= \varphi^\Box \vee \psi^\Box \\ (\varphi \rightarrow \psi)^\Box &:= \Box(\varphi^\Box \rightarrow \psi^\Box) \end{aligned} \quad \square$$

Faz-se interessante pontuar que as traduções \bullet° e \bullet^\Box correspondem, respectivamente, às traduções \bullet° e \bullet^* do sistema intuicionista ao sistema linear providas por Girard (1987), 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*). Ademais, as duas traduções providas são equivalentes, conforme demonstrado pelo teorema **T₂**.

Lema 1. $\vdash (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma) \rightarrow \alpha \rightarrow \beta \wedge \gamma$.

Lema 2. $\vdash \Box(\alpha \wedge \beta) \rightarrow \Box\alpha \wedge \Box\beta$.

Demonstração. Pode ser provado pela seguinte sucessão de dedução:

| | |
|---|---|
| 1 | $\alpha \wedge \beta \rightarrow \alpha$ |
| 2 | $\Box(\alpha \wedge \beta \rightarrow \alpha)$ |
| 3 | $\Box(\alpha \wedge \beta \rightarrow \alpha) \rightarrow (\Box(\alpha \wedge \beta) \rightarrow \Box\alpha)$ |
| 4 | $\Box(\alpha \wedge \beta) \rightarrow \Box\alpha$ |

| | |
|----|--|
| 5 | $\alpha \wedge \beta \rightarrow \beta$ |
| 6 | $\Box(\alpha \wedge \beta \rightarrow \beta)$ |
| 7 | $\Box(\alpha \wedge \beta \rightarrow \beta) \rightarrow (\Box(\alpha \wedge \beta) \rightarrow \Box\beta)$ |
| 8 | $\Box(\alpha \wedge \beta) \rightarrow \Box\beta$ |
| 9 | $(\Box(\alpha \wedge \beta) \rightarrow \Box\alpha) \rightarrow (\Box(\alpha \wedge \beta) \rightarrow \Box\beta) \rightarrow \Box(\alpha \wedge \beta) \rightarrow \Box\alpha \wedge \Box\beta$ |
| 10 | $(\Box(\alpha \wedge \beta) \rightarrow \Box\beta) \rightarrow \Box(\alpha \wedge \beta) \rightarrow \Box\alpha \wedge \Box\beta$ |
| 11 | $\Box(\alpha \wedge \beta) \rightarrow \Box\alpha \wedge \Box\beta$ |

□

Lema 3. $\vdash \Box\alpha \wedge \Box\beta \rightarrow \Box(\alpha \wedge \beta)$.

Lema 4. $\vdash \Box(\alpha \rightarrow \beta) \rightarrow \Box\alpha \rightarrow \Box\beta$.

Teorema 6. $\forall \alpha \in \mathcal{L}_I . \Box\alpha^\circ \leftrightarrow \alpha^\Box$.

Demonstração. Prova por indução na profundidade de α .

Caso 1 (Base). Para $|\alpha| = 0$, existem dois casos a serem considerados.

Caso 1.1 ($\alpha = a$). $a^\circ = a$ e $a^\Box = \Box a$, assim $\Box a^\circ = a^\Box$ e, portanto, $\Box a^\circ \leftrightarrow a^\Box$.

Caso 2.1 ($\alpha = \perp$). $\perp^\circ = \perp$ e $\perp^\Box = \perp$. A ida $\Box\perp \rightarrow \perp$ consiste em um axioma, sendo, portando provada trivialmente pela sucessão de dedução $\langle \Box\perp \rightarrow \perp \rangle$. A volta $\perp \rightarrow \Box\perp$ equivale a provar, por meio do teorema da dedução, que $\{\perp\} \vdash_{\mathbf{M}} \Box\perp$, o que pode ser provado trivialmente pela sucessão de dedução $\langle \perp, \Box\perp \rangle$, que consiste na invocação da premissa e aplicação da regra da necessitação, nessa ordem.

Caso 2 (Passo). No passo, deve-se demonstrar que, caso $\Box\alpha^\circ \leftrightarrow \alpha^\Box$ para $|\alpha| = n$, então $\Box\alpha^\circ \leftrightarrow \alpha^\Box$ para $|\alpha| = n + 1$, onde $n \in \mathbb{N}$. Assim, seja $\Box\alpha^\circ \leftrightarrow \alpha^\Box$ uma proposição verdadeira para $|\alpha| = k$, onde $k \in \mathbb{N}$. Existem os seguintes casos a serem considerados para $|\alpha| = k + 1$.

Caso 2.1. Caso $\alpha = \varphi \wedge \psi$, sabe-se que $\Box(\varphi \wedge \psi)^\circ = \Box(\varphi^\circ \wedge \psi^\circ)$ e $(\varphi \wedge \psi)^\Box = \varphi^\Box \wedge \psi^\Box$. Pelo lemas **L2** e **L3** temos que $\Box(\varphi^\circ \wedge \psi^\circ) \leftrightarrow \Box\varphi^\circ \wedge \Box\psi^\circ$ e pela premissa da indução temos que $\Box\varphi^\circ \leftrightarrow \varphi^\Box$ e $\Box\psi^\circ \leftrightarrow \psi^\Box$. Deste modo, $\Box(\varphi \wedge \psi)^\circ \leftrightarrow (\varphi \wedge \psi)^\Box$.

Caso 2.2. Caso $\alpha = \varphi \vee \psi$, sabe-se que $\Box(\varphi \vee \psi)^\circ = \Box(\Box\varphi^\circ \vee \Box\psi^\circ)$ e $(\varphi \vee \psi)^\Box = \varphi^\Box \vee \psi^\Box$. Para a ida, basta aplicar o axioma **B2**. Para a volta, basta aplicar a regra da necessitação.

Caso 2.3. Caso $\alpha = \varphi \rightarrow \psi$, sabe-se que $\Box(\varphi \rightarrow \psi)^\circ = \Box(\Box\varphi^\circ \rightarrow \psi^\circ)$ e $(\varphi \rightarrow \psi)^\Box = \Box(\varphi^\Box \rightarrow \psi^\Box)$. Para a ida, basta aplicar o axioma **B₁**. Para a volta, basta aplicar o lema **L₄** seguido pela necessitação. \square

3.3 Corretude

Teorema 7. $\forall \alpha \in \mathcal{L}_{\mathbf{I}} . \Gamma \vdash_{\mathbf{I}} \alpha \Rightarrow \Gamma^\Box \vdash_{\mathbf{M}} \alpha^\Box$

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 (A₁). Deve-se demonstrar que $\vdash \Box(\alpha^\Box \rightarrow \Box(\beta^\Box \rightarrow \alpha^\Box))$. Pelo teorema **T₁**, basta provar que $\{\alpha^\Box, \beta^\Box\} \vdash \alpha^\Box$, o que pode ser feito pela seguinte sucessão de dedução:

| | | |
|---|---------------|----------|
| 1 | α^\Box | P |
|---|---------------|----------|

Caso 2.2 (A₂).

| | | |
|---|---|---|
| 1 | $\Box(\alpha^\Box \rightarrow \beta^\Box) \rightarrow \alpha^\Box \rightarrow \beta^\Box$ | B₂ |
| 2 | $\Box(\alpha^\Box \rightarrow \beta^\Box)$ | P |
| 3 | $\alpha^\Box \rightarrow \beta^\Box$ | R₁ $\langle 1, 2 \rangle$ |
| 4 | α^\Box | P |
| 5 | β^\Box | R₁ $\langle 3, 4 \rangle$ |
| 6 | $\Box(\alpha^\Box \rightarrow \Box(\beta^\Box \rightarrow \alpha^\Box)) \rightarrow \alpha^\Box \rightarrow \Box(\beta^\Box \rightarrow \alpha^\Box)$ | B₂ |
| 7 | $\Box(\alpha^\Box \rightarrow \Box(\beta^\Box \rightarrow \alpha^\Box))$ | P |
| 8 | $\alpha^\Box \rightarrow \Box(\beta^\Box \rightarrow \alpha^\Box)$ | R₁ $\langle 6, 7 \rangle$ |
| 9 | $\Box(\beta^\Box \rightarrow \alpha^\Box)$ | R₁ $\langle 4, 8 \rangle$ |

| | | |
|----|---|--|
| 10 | $\Box(\beta^\Box \rightarrow \alpha^\Box) \rightarrow \beta^\Box \rightarrow \gamma^\Box$ | B₂ |
| 11 | $\beta^\Box \rightarrow \gamma^\Box$ | R₁ $\langle 10, 9 \rangle$ |
| 12 | γ^\Box | R₁ $\langle 11, 5 \rangle$ |

Caso 2.3 (A₃).

| | | |
|---|--|---|
| 1 | $\alpha^\Box \rightarrow \beta^\Box \rightarrow \alpha^\Box \wedge \beta^\Box$ | A₃ |
| 2 | α^\Box | P |
| 3 | $\beta^\Box \rightarrow \alpha^\Box \wedge \beta^\Box$ | R₁ $\langle 1, 2 \rangle$ |
| 4 | β^\Box | P |
| 5 | $\alpha^\Box \wedge \beta^\Box$ | R₁ $\langle 3, 4 \rangle$ |

Caso 2.4 (A₄). Deve-se demonstrar que $\vdash \Box(\alpha^\Box \wedge \beta^\Box \rightarrow \alpha^\Box)$, o que pode ser feito ela seguinte sucessão de dedução:

| | | |
|---|---|--|
| 1 | $\alpha^\Box \wedge \beta^\Box \rightarrow \alpha^\Box$ | A₄ |
| 2 | $\Box(\alpha^\Box \wedge \beta^\Box \rightarrow \alpha^\Box)$ | R₂ $\langle 1 \rangle$ |

Caso 2.5 (A₅). Deve-se demonstrar que $\vdash \Box(\alpha^\Box \wedge \beta^\Box \rightarrow \beta^\Box)$, o que pode ser feito ela seguinte sucessão de dedução:

| | | |
|---|--|--|
| 1 | $\alpha^\Box \wedge \beta^\Box \rightarrow \beta^\Box$ | A₅ |
| 2 | $\Box(\alpha^\Box \wedge \beta^\Box \rightarrow \beta^\Box)$ | R₂ $\langle 1 \rangle$ |

Caso 2.6 (A₆). Deve-se demonstrar que $\vdash \Box(\alpha^\Box \rightarrow \alpha^\Box \vee \beta^\Box)$, o que pode ser feito ela seguinte sucessão de dedução:

| | | |
|---|---|--|
| 1 | $\alpha^\Box \rightarrow \alpha^\Box \vee \beta^\Box$ | A₆ |
| 2 | $\Box(\alpha^\Box \rightarrow \alpha^\Box \vee \beta^\Box)$ | R₂ $\langle 1 \rangle$ |

Caso 2.7 (A₇). Deve-se demonstrar que $\vdash \Box(\beta^\Box \rightarrow \alpha^\Box \vee \beta^\Box)$, o que pode ser feito ela seguinte sucessão de dedução:

| | | |
|---|--|--|
| 1 | $\beta^\Box \rightarrow \alpha^\Box \vee \beta^\Box$ | A₇ |
| 2 | $\Box(\beta^\Box \rightarrow \alpha^\Box \vee \beta^\Box)$ | R₂ $\langle 1 \rangle$ |

Caso 2.8 ($\mathbf{A_8}$). Deve-se demonstrar que $\vdash (\alpha^\square \rightarrow \gamma^\square) \rightarrow (\beta^\square \rightarrow \gamma^\square) \rightarrow \alpha^\square \vee \beta^\square \rightarrow \gamma^\square$. Pelo teorema $\mathbf{T_1}$, basta provar que $\{\alpha \rightarrow \gamma, \beta \rightarrow \gamma, \alpha \vee \beta\} \vdash \alpha^\square$, o que pode ser feito pela seguinte sucessão de dedução:

| | | |
|----|---|--------------------------------------|
| 1 | $(\alpha^\square \rightarrow \gamma^\square) \rightarrow (\beta^\square \rightarrow \gamma^\square) \rightarrow \alpha^\square \vee \beta^\square \rightarrow \gamma^\square$ | $\mathbf{A_8}$ |
| 2 | $\Box(\alpha^\square \rightarrow \gamma^\square) \rightarrow \alpha^\square \rightarrow \gamma^\square$ | $\mathbf{B_2}$ |
| 3 | $\Box(\alpha^\square \rightarrow \gamma^\square)$ | \mathbf{P} |
| 4 | $\alpha^\square \rightarrow \gamma^\square$ | $\mathbf{R_1} \langle 2, 3 \rangle$ |
| 5 | $(\beta^\square \rightarrow \gamma^\square) \rightarrow \alpha^\square \vee \beta^\square \rightarrow \gamma^\square$ | $\mathbf{R_1} \langle 1, 4 \rangle$ |
| 6 | $\Box(\beta^\square \rightarrow \gamma^\square) \rightarrow \beta^\square \rightarrow \gamma^\square$ | $\mathbf{B_2}$ |
| 7 | $\Box(\beta^\square \rightarrow \gamma^\square)$ | \mathbf{P} |
| 8 | $\beta^\square \rightarrow \gamma^\square$ | $\mathbf{R_1} \langle 6, 7 \rangle$ |
| 9 | $\alpha^\square \vee \beta^\square \rightarrow \gamma^\square$ | $\mathbf{R_1} \langle 5, 8 \rangle$ |
| 10 | $\alpha^\square \vee \beta^\square$ | \mathbf{P} |
| 11 | γ^\square | $\mathbf{R_1} \langle 9, 10 \rangle$ |

Caso 2.9 ($\mathbf{A_\perp}$). Deve-se demonstrar que $\vdash \Box(\perp \rightarrow \alpha^\square)$. Pelo teorema $\mathbf{T_1}$, basta provar que $\{\perp\} \vdash \alpha^\square$, o que pode ser feito pela seguinte sucessão de dedução:

| | | |
|---|---|-------------------------------------|
| 1 | $((\alpha^\square \rightarrow \perp) \rightarrow \perp) \rightarrow \alpha^\square$ | $\mathbf{A_\neg}$ |
| 2 | $\perp \rightarrow (\alpha^\square \rightarrow \perp) \rightarrow \perp$ | $\mathbf{A_1}$ |
| 3 | \perp | \mathbf{P} |
| 4 | $(\alpha^\square \rightarrow \perp) \rightarrow \perp$ | $\mathbf{R_1} \langle 2, 3 \rangle$ |
| 5 | α^\square | $\mathbf{R_1} \langle 1, 4 \rangle$ |

Caso 2.9 ($\mathbf{R_1}$). Deve-se demonstrar que, se $\vdash \Box(\alpha^\square \rightarrow \beta^\square)$ ($\mathbf{H_1}$) e $\vdash \alpha^\square$ ($\mathbf{H_2}$), então β^\square . Isso pode ser feito pela seguinte sucessão de dedução:

| | | |
|---|---|-------------------------------------|
| 1 | $\Box(\alpha^\square \rightarrow \beta^\square) \rightarrow \alpha^\square \rightarrow \beta^\square$ | $\mathbf{B_2}$ |
| 2 | $\Box(\alpha^\square \rightarrow \beta^\square)$ | $\mathbf{H_1}$ |
| 3 | $\alpha^\square \rightarrow \beta^\square$ | $\mathbf{R_1} \langle 1, 2 \rangle$ |
| 4 | α^\square | $\mathbf{H_2}$ |
| 5 | β^\square | $\mathbf{R_1} \langle 3, 4 \rangle$ |

□

3.4 Completude

BABIRESKI: Não vai rolar de provar a completude como Troelstra and Schwichtenberg (2000). Vou precisar procurar outros artigos.

Referências Bibliográficas

Patrick Blackburn, Maarten de Rijke, and Yde Venema. *Modal logic*. Cambridge University Press, 2001.

Jean-Yves Béziau. Universal logic. *Logica*, 1994.

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

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

Raul Hakli and Sara Negri. Does the deduction theorem fail for modal logic? *Synthese*, 2012.

Ruth Barcan Marcus. Strict implication, deducibility and the deduction theorem. *The Journal of Symbolic Logic*, 1953.

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

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

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

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

Richard Zach. Box and diamonds: an open introduction to modal logic, 2024.