Sobre as lógicas linear, intuicionista e clássica e suas especificações.

Aluno: Wesley Luiz Alves da Mata
Orientadora: Elaine Gouvêa Pimentel

Departamento de Matemática
Universidade Federal de Minas Gerais, Belo Horizonte, MG.

21 de setembro de 2011

Sumário

Lista de Figuras

1 Introdução

A presente dissertação visa o estudo de três lógicas, as lógicas clássica, intuicionista e linear, bem como suas especificações, necessárias para a construção do provador automático de teoremas PLLIC, que verifica quando seqüentes do tipo $\Gamma \vdash_L \Delta$ são prováveis, onde Γ, Δ são conjuntos de fórmulas e L pode ser uma das seguintes lógicas: linear LL, intuicionista LJ ou clássica LK. Apesar de ser possível expandir o programa para o uso de quantificadores (universal e existencial), PLLIC decide sobre a provabilidade do fragmento *proposicional* das lógicas acima citadas, uma vez que a nossa intenção é que o programa sempre pare, ou seja, que a pergunta: *o seqüente* $\Gamma \vdash_L \Delta$ *é provável?* tenha sempre uma resposta: *sim* ou *não*. Além disso, se um seqüente é provável, PLLIC exibe a sua prova em cálculo de seqüentes.

Iniciaremos nossos estudos pela descrição da lógica de primeira ordem introduzindo noções de tipos, assinaturas, termos, fórmulas e apresentando um sistema de provas baseado no cálculo de seqüentes introduzido por Gerhad Gentzen, denominado sistema G.

Na seção seguinte faremos um estudo da lógica clássica. E com o intuito de eliminar problemas computacionais, existentes na especificação do sistema criado por Gentzen, construiremos um sistema equivalente eliminando tais problemas. Em seguida faremos um estudo semântico da lógica clássica identificando uma ligação com a álgebra de Boole e com a topologia.

Na seção 4 apresentaremos uma variação do sistema G para a lógica intuicionista e novamente por razões computacionais construiremos um sistema equivalente. No campo semântico veremos que esta lógica pode ser interpretada como uma álgebra de Heyting.

Posteriormente demonstraremos a propriedade de $Cut - elimination$ do sistema G.

E para encerrar, apresentaremos a lógica linear e o sistema $Forum$ proposto por Dale Miller, no qual fórmulas são construidas utilizando apenas os conectivos assíncronos junto com a versão intuicionista da implicação, permitindo assim, a especificação da lógica linear.

2 Lógica de Primeira Ordem

Começaremos por descrever a Lógica de Primeira Ordem, que é um sistema de argumentação simbólica em que cada sentença ou afirmativa é composta de *sujeitos* e *predicados*. São exemplos de predicados: "*todo homem é mortal*", "*p ou não p*" e "*para todo n, a soma de n e zero é n*".

Os predicados a serem utilizados na prática dependem do problema específico no qual estamos trabalhando. Dos exemplos de predicado acima, o primeiro é o clássico exemplo estudado por Aristóteles; o segundo é a fórmula lógica que aparece no famoso princípio do terceiro excluído, sobre o qual falaremos mais tarde; e o último... bem, depende de quem é n! Caso n seja um número natural, o predicado define o caso base da soma de números naturais. Já se n é um número real, estamos simplesmente dizendo que a soma de zero com um número qualquer n é o próprio n. Desta forma, para cada predicado devemos descrever o seu *tipo*.

Começaremos portanto por descrever a noção de tipos e assinaturas, que são conjuntos finitos de constantes, cada uma com seu tipo definido. Passaremos então a definir a sintaxe da lógica de primeira ordem, isto é, como podemos construir *fórmulas* a partir de predicados atômicos e alguns conectivos. Por fim, detalharemos um *sistema de provas* baseado em *cálculo de seqüentes* para a lógica de primeira ordem.

2.1 Tipos e Assinaturas

Tipos estão presentes tanto em matemática (e portanto em lógica matemática) quanto em computação. Na teoria de conjuntos tradicional, o agrupamento de elementos em um conjunto independe da natureza desses elementos. Quando passamos a trabalhar em aplicações específicas, precisamos classificar os objetos em categorias, de acordo com o seu uso ou aplicação.

A noção de tipos origina-se dessa classificação: um tipo é uma coleção de objetos ou valores que possuem alguma propriedade em comum.

Seja S um conjunto fixo, finito de tipos primitivos. O conjunto de tipos primitivos que tomamos depende do tipo de problema que queremos resolver, ou do tipo de aplicação que estamos interessados.

Por exemplo, em linguagens de programação tipadas existem alguns tipos pré-definidos, implícitos. Alguns tipos comuns em linguagens de programação são, por exemplo, o tipo primitivo `int`, o tipo primitivo `real` e o tipo primitivo `string`. Na sintaxe do λ-*Prolog* [20], escrevemos

```
kind   int      type.
kind   real     type.
```

```
kind   string   type.
```

para representar que `int`, `real` e `string` são tipos.

No caso de linguagens de programação *lógicas* como Prolog ou λ-Prolog, existe um tipo primitivo relativo a predicados, o tipo `o` (veja Church [5]):

```
kind   o        type.
```

No presente texto, assumiremos que `o` é sempre membro de S.

O *conjunto dos tipos* T é o menor conjunto de expressões que contenha os tipos primitivos S e seja fechado com relação à construção de tipos funcionais, construídos com o símbolo binário infixado $\rightarrow$. Ou seja, tipos de T são dados pela sintaxe abaixo:

Tipos	$\tau ::=$	$\tau,\ \tau \in S$	tipo primitivo
		$\tau_1 \rightarrow \tau_2$	tipo funcional

Figura 1: Sintaxe de tipos

Utilizaremos letras gregas τ e σ para representar variáveis sintáticas para tipos. Como de maneira usual, o construtor de tipos $\rightarrow$ associa-se à direita: lê-se $\tau_1 \rightarrow \tau_2 \rightarrow \tau_3$ como $\tau_1 \rightarrow (\tau_2 \rightarrow \tau_3)$.

Seja τ o tipo $\tau_1 \rightarrow \tau_2 \rightarrow \ldots \rightarrow \tau_n \rightarrow \tau_0$ onde τ_0 é um tipo primitivo (ou seja, $\tau_0 \in S$) e $n \geq 0$. Os tipos $\tau_1, \ldots, \tau_n$ são ditos *tipos domínio* de τ enquanto que o tipo τ_0 é chamado *tipo imagem* de τ.

Exemplo 1 *Suponha que estejamos interessados em saber se um determinado aluno teve um desempenho ruim durante o semestre, como descrito abaixo:*

```
kind pessoa type.

type a                           pessoa.
type professor, naoestudou       pessoa -> o.
type desempenhoruim              pessoa -> o.
type aluno, naopassou            pessoa -> pessoa -> o.

desempenhoruim X :- pi y\(professor y =>aluno X y => naopassou X y).
naopassou A B :- professor B, aluno A B, naoestudou A.

naoestudou a.
```

```
% Pergunta-se: ?- desempenhoruim a.
```

O código acima retrata a situação em que um aluno possui um desempenho ruim se para toda[1] *disciplina que ele cursa ele não passa. E um estudante não passa se ele não estuda.*

O único tipo primitivo para este exemplo é `pessoa`*, que pertence ao conjunto* S *juntamente com o tipo* `o`.

Os predicados `professor, naoestudou, naopassou, desempenhoruim` *e* `aluno` *possuem tipos funcionais.*

Um conceito muito importante é o de *ordem* de um tipo.

Definição 1 *A* ***ordem*** *de um tipo* τ *(representado por* $ord(\tau)$*) é definida da seguinte forma:*

$$\begin{array}{lcl} ord(\tau) & = & 0 \ se \ \tau \in S \\ ord(\tau_1 \rightarrow \tau_2) & = & max\{ord(\tau_1) + 1, ord(\tau_2)\} \end{array}$$

No Exemplo 1, o tipo primitivo `pessoa` possui ordem 0 pois pertence ao conjunto S. Se chamamos $\tau = pessoa \rightarrow \mathtt{o}$, então

$$\begin{array}{lcl} ord(\tau) & = & max\{ord(pessoa) + 1, ord(\mathtt{o})\} \\ & = & max\{0 + 1, 0\} \\ & = & 1. \end{array}$$

Por sua vez, se $\tau' = pessoa \rightarrow pessoa \rightarrow \mathtt{o}$, então

$$\begin{array}{lcl} ord(\tau') & = & max\{ord(pessoa) + 1, ord(\tau)\} \\ & = & max\{0 + 1, 1\} \\ & = & 1. \end{array}$$

Fica claro então por indução que se $\tau = \tau_1 \rightarrow \ldots \rightarrow \tau_n \rightarrow \tau_0$ onde $\tau_0, \tau_1, \ldots, \tau_n \in S$, então $ord(\tau) = 1$.

Definição 2 *Os tipos* τ *de ordem 0 ou 1, tais que nenhum tipo argumento de* τ *é* `o`*, são chamados de* ***tipos de primeira ordem****.*

Desta forma, todos os predicados definidos no Exemplo 1 possuem tipo de primeira ordem.

[1]Em λ-Prolog, representamos *para todo* x como `pi x\`.

Como de maneira usual, assumimos que para cada tipo τ existam inúmeras constantes e variáveis deste tipo. Também constantes e variáveis não se sobrepõem, e se duas constantes ou variáveis têm tipos diferentes, são constantes ou variáveis diferentes.

Uma assinatura Σ sobre S é um conjunto finito de constantes. Representaremos Σ listando seus membros como pares da forma $a : \tau$, onde a é uma constante de tipo τ. Uma assinatura é de primeira ordem se todas suas constantes possuem tipos de primeira ordem.

2.2 Termos e fórmulas de primeira ordem

Agora podemos definir a sintaxe da lógica de primeira ordem $\mathcal{F}$. As constantes lógicas de $\mathcal{F}$ são os símbolos apresentados na tabela abaixo:

Constante lógica	**Símbolo**
conjunção	$\wedge$
disjunção	$\vee$
implicação	$\supset$
verdadeiro	$\top$
falso	$\bot$
quantificação universal	$\forall_\tau$
quantificação existencial	$\exists_\tau$
negação	$\neg$

onde $\tau \in S - \{\mathtt{o}\}$.
Por questões didáticas, incluiremos também a negação como constante lógica. Como veremos mais adiante, $\neg B$ é equivalente a $B \supset \bot$.

Exemplo 2 *Utilizando a sintaxe de λ-Prolog, a assinatura Σ de $\mathcal{F}$ pode ser especificada como:*

```
kind  form          type.
kind  i             type.

type  true, false   form.
type  neg           form -> form.
type  and, or, imp  form -> form -> form.
type  forall        (i -> form) -> form.
type  exists        (i -> form) -> form.
```

Definição 3 *A função* ***aridade*** *associa a cada símbolo de função ou de predicado o número de argumentos da respectiva função ou predicado.*

Os símbolos de função de aridade 0 são designados *símbolos de constantes*. Os símbolos de predicado de aridade 0 são designados *símbolos proposicionais*.

Passaremos agora a descrever algumas noções seguindo as definições apresentadas em [17].

Definição 4 *Seja τ um tipo da forma $\tau_1 \to \tau_2 \to \ldots \to \tau_n \to \tau_0$ onde τ_0 é um tipo primitivo e $n \geq 0$.*

i. Se τ_0 for `o`*, uma constante do tipo τ é uma **constante de predicado** de aridade n.*

ii. Se τ_0 não for `o`*, então uma constante do tipo τ é ou uma **constante individual** se $n = 0$, ou é uma **constante funcional** de aridade n se $n \geq 1$.*

No Exemplo 1, `a` é uma constante individual, `professor, naoestudou` e `desempenhoruim` são constantes de predicado de aridade 1 enquanto que `aluno` e `naopassou` são constantes de predicado de aridade 2.

No Exemplo 2, $\top$ (true) e $\perp$ (false) são constantes individuais, `neg` é uma constante funcional de aridade 1, enquanto `and, or` e `imp` são constantes funcionais de aridade 2.

De maneira similar, podemos definir variável de predicado de aridade n, variável individual e variável funcional de aridade n.

Definição 5 *Seja τ um tipo primitivo diferente de* `o`*. Um t**ermo de primeira ordem** de tipo τ pode ser: ou uma constante c, ou uma variável X de tipo τ, ou da forma $f\ t_1 \ldots t_n$ onde f é uma constante funcional de tipo $\tau_1 \to \cdots \to \tau_n \to \tau$. Neste caso, dizemos que f é a* cabeça *e $t_1 \ldots t_n$ são os* argumentos *do termo.*

Em outras palavras, termos de primeira ordem são dados pela gramática:

$$t \ ::= \ c \mid X \mid f\ t_1 \ldots t_n$$

Definição 6 *Uma* fórmula de primeira ordem *pode ser atômica ou não-atômica.*

*i. Uma **fórmula atômica** é da forma $p\ t_1 \ldots t_n$ onde $n \geq 0$, p é uma constante de predicado de tipo $\tau_1 \to \cdots \to \tau_n \to o$, e $t_1, \ldots, t_n$ são termos de primeira ordem de tipos $\tau_1, \ldots, \tau_n$, respectivamente. A constante de predicado p é a cabeça desta fórmula atômica.*

ii. ***Fórmulas não-atômicas*** *de $\mathcal{F}$ são dadas pela gramática*

$$F \quad ::= \quad (F \wedge F) \mid (F \vee F) \mid (F \supset F) \mid \bot \mid \top \mid \forall_\tau x.F \mid \exists_\tau x.F$$

onde τ é um tipo primitivo diferente de `o`*.*

Exemplo 3 *Seguindo o trabalho de especificação da lógica de primeira ordem, podemos descrever fórmulas atômicas e não atômicas:*

```
nao_atomico (A imp B).
nao_atomico (A and B).
nao_atomico (A or B).
nao_atomico false.
nao_atomico true.
nao_atomico (neg A).
nao_atomico (forall B).
nao_atomico (exists B).

atomico B :- not (nao_atomico B).
```

Observe que `nao_atomico` *e* `atomico` *são predicados de tipo*

```
form -> o
```

e que `not` *é a negação do λ-Prolog.*

2.3 Cálculo de Seqüentes

Um sistema lógico formal é composto, além da sintaxe (ou notação, como a que acabamos de apresentar), de uma especificação cuidadosa de regras de argumentação (regras de inferência) e de alguma noção de como interpretar e dar um significado as sentenças (ou proposições) da linguagem adotada (semântica).

Na presente seção, apresentaremos um sistema de provas baseado em cálculo de seqüentes para a lógica de primeira ordem $\mathcal{F}$. Chamaremos tal sistema de **G**, seguindo a notação de [34], e em homenagem a Gentzen.

Foi o alemão Gerhard Gentzen que introduziu o cálculo de seqüentes nos anos 1930[2] [8], cálculo este que permite lidar com verdades lógicas considerando a forma da dedução.

[2] Gentzen que também introduziu o sistema de *dedução natural* – para uma introdução ao sistema de dedução natural, veja [27] ou [25].

Um seqüente de $\mathcal{F}$ é uma tripla:

$$\Sigma : \Gamma \vdash \Delta$$

onde Σ é uma assinatura de primeira ordem sobre S, Γ e Δ são multi-conjuntos finitos (possivelmente vazios) de fórmulas e $\vdash$ é um meta-símbolo de validade. Chamamos Γ de *antecedente* e Δ de *sucedente* do seqüente. Como de costume, denotaremos a união $\Gamma \cup \{B\}$ por Γ, B. Em geral, também omitiremos a assinatura, escrevendo um sequente simplesmente como: $\Gamma \vdash \Delta$.

Uma prova para o seqüente $\Gamma \vdash \Delta$ é uma *árvore finita* cuja *raiz* é o próprio seqüente, os *galhos* são construídos usando as regras de inferência, e as *folhas* são instâncias do único axioma do cálculo, o axioma inicial (Figura 2).

As regras de inferência de **G**, por sua vez, podem ser separadas em três grupos: o único axioma do sistema (Figura 2), as regras de introdução de conectivos lógicos (Figura 3) as regras estruturais (Figura 4), entre elas a regra *cut* (de corte) sobre a qual falaremos mais tarde.

Vamos descrever agora alguns exemplos de provas utilizando cálculo de sequentes. Começaremos por mostrar que, na lógica de primeira ordem, a negação de uma fórmula B é equivalente a $B \supset \perp$,

Exemplo 4 *Demonstrar a equivalência $\neg B \equiv B \supset \perp$, significa provar que $\neg B \vdash B \supset \perp$ e $B \supset \perp \vdash \neg B$:*

- $\neg B \vdash B \supset \perp$:

$$\dfrac{\dfrac{\dfrac{}{B \vdash B}\ Inicial}{\neg B, B \vdash \perp}\ \neg L}{\neg B \vdash B \supset \perp}\ \supset R$$

- $B \supset \perp \vdash \neg B$:

$$\dfrac{\dfrac{\dfrac{}{B \vdash B}\ Inicial \qquad \dfrac{}{\perp \vdash \perp}\ \perp L}{B \supset \perp, B \vdash \perp}\ \supset L}{B \supset \perp \vdash \neg B}\ \neg R$$

Outro exemplo importante é o princípio do terceiro excluído.

Exemplo 5 *Na lógica clássica de primeira ordem (veja Seção 3) vale o tão comentado* princípio do terceiro excluído. *Ou seja, a proposição*

$$p \vee \neg p$$

é sempre válida. Isso significa que uma fórmula é sempre ou verdadeira, ou falsa.

$$\frac{}{A \vdash A}\ \mathit{Inicial}$$

Figura 2: Axioma inicial de **G**

$$\frac{}{\Gamma \vdash \top, \Delta}\ \top R \qquad \frac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash A \wedge B, \Delta_1, \Delta_2}\ \wedge R$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \supset B, \Delta}\ \supset R \qquad \frac{\Gamma, A \vdash \bot, \Delta}{\Gamma \vdash \neg A, \Delta}\ \neg R$$

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \vee \mathit{R1} \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \vee \mathit{R2}$$

$$\frac{}{\Gamma, \bot \vdash \Delta}\ \bot L \qquad \frac{\Gamma_1 \vdash A, \Delta_1}{\Gamma_1, \Gamma_2, \neg A \vdash \Delta_1, \Delta_2}\ \neg L$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge \mathit{L1} \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge \mathit{L2}$$

$$\frac{\Gamma_1, A \vdash \Delta_1 \quad \Gamma_2, B \vdash \Delta_2}{\Gamma_1, \Gamma_2, A \vee B \vdash \Delta_1, \Delta_2}\ \vee L \qquad \frac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2, B \vdash \Delta_2}{\Gamma_1, \Gamma_2, A \supset B \vdash \Delta_1, \Delta_2}\ \supset L$$

Figura 3: Regras de introdução de **G**

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ \mathit{weak}\ L \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}\ \mathit{weak}\ R$$

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ \mathit{cont}\ L \qquad \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}\ \mathit{cont}\ R$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad A, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ \mathit{Cut}$$

Figura 4: Regras estruturais de **G**

Essa afirmação é (extremamente) não construtiva, uma vez que nada se pode dizer sobre qual das opções é valida. A prova em cálculo de seqüentes no sistema **G** *é dada abaixo:*

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{p \vdash p}\ Inicial}{p \vdash \bot, p}\ weakR}{\vdash p, \neg p}\ \neg R}{\vdash p, p \vee \neg p}\ \vee R2}{\vdash p \vee \neg p, p \vee \neg p}\ \vee R1}{\vdash p \vee \neg p}\ contR$$

Observe que esta prova só é possível porque podemos utilizar regras estruturais à direita do seqüente. Desta forma, evitamos escolher entre provar p *ou* $\neg p$*, simplesmente através da duplicação do sucedente. Como veremos na Seção 4, a proposição* $p \vee \neg p$ *não pode ser provada na lógica intuicionista.*

O cálculo de seqüentes possui uma série de características interessantes:

- possui apenas regras de introdução para conectivos, isto é, regras que, quando lidas de cima para baixo (*top-down*), introduzem um conectivo lógico;
- premissas e conclusões são tratadas da mesma forma e são construídas simultaneamente;
- é tecnicamente bem simples: quando lidas de baixo pra cima (*bottom up*), fica claro que as regras no cálculo de seqüentes simplificam o processo de construção de provas.

Desta forma, é fácil especificar todas as regras de introdução descritas nas Figuras 2 e 3. O axioma inicial também é facilmente especificado. Acontece que a presença de regras estruturais pode trazer alguns problemas de implementação. Por exemplo, a implementação de *contraction* (contração) é inviável, uma vez que geraria loops.

Não existe um sistema único de provas sem regras estruturais que represente ambas as lógicas clássica e intuicionista. Desta forma, a partir deste ponto vamos dividir a nossa discussão de acordo com a lógica em questão, com exceção da regra *cut*, que será analisada na Seção 3.2.

3 Lógica clássica

Construiremos um sistema de provas conveniente para a lógica clássica substituindo o sistema **G** dado pelas regras nas Figuras 2, 3 e 4 pelo sistema apresentado na Figura 5, que chamaremos de **G3c**, ainda seguindo [34].

$$\frac{}{\Gamma, A \vdash \Delta, A}\ \textit{Inicial}$$

$$\frac{}{\Gamma \vdash \top, \Delta}\ \top R \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ \wedge R$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \supset B, \Delta}\ \supset R \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \vee R$$

$$\frac{}{\Gamma, \bot \vdash \Delta}\ \bot L \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge L$$

$$\frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ \vee L \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \supset B \vdash \Delta}\ \supset L$$

Figura 5: Sistema **G3c** para a lógica clássica de primeira ordem

Note que no sistema **G3c** as regras de inferência para o conectivo lógico $\neg$ não são apresentadas. Pois, assim como no sistema **G** tem-se que $\neg B \equiv B \supset \bot$ (Veja exemplo 4). Sendo assim, as regras de inferência da negação podem ser simuladas pelas regras da implicação e portanto, removidas do sistema.

3.1 Equivalência de sistemas

Observe que podemos simular a regra $\vee R$ da Figura 5 utilizando as regras $\vee R1$ e $\vee R2$ da Figura 3, na presença da regra *contraction* (Figura 4). De fato,

$$\cfrac{\cfrac{\cfrac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A, A \vee B}\ \vee R2}{\Gamma \vdash \Delta, A \vee B, A \vee B}\ \vee R1}{\Gamma \vdash \Delta, A \vee B}\ contR$$

Por outro lado, não há um jeito de simular as regras $\vee R1$ e $\vee R2$ em **G3c** uma vez que não podemos utilizar *weakening* (enfraquecimento) explicitamente. Mas a ocorrência desta regra implícita no axioma inicial faz com que, para cada prova de um certo seqüente em **G** tal que as regras $\vee R1$ e/ou $\vee R2$

sejam aplicadas, exista uma outra prova do mesmo seqüente em **G3c** tal que a regra $\vee R$ seja aplicada.

Antes de demonstrar essa afirmação, iremos ilustrá-la em um exemplo.

Exemplo 6 *Considere a seguinte prova em* **G***:*

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\,Inicial}{A \vdash B \vee A}\,\vee R2 \qquad \dfrac{\dfrac{}{B \vdash B}\,Inicial}{B \vdash B \vee A}\,\vee R1}{A \vee B \vdash B \vee A}\,\vee L$$

Podemos construir uma prova similar em **G3c***:*

$$\dfrac{\dfrac{\dfrac{}{A \vdash B, A}\,Inicial}{A \vdash B \vee A}\,\vee R \qquad \dfrac{\dfrac{}{B \vdash B, A}\,Inicial}{B \vdash B \vee A}\,\vee R}{A \vee B \vdash B \vee A}\,\vee L$$

Observe que, para terminar a prova, basta que a mesma fórmula esteja tanto no antecedente quanto no sucedente do seqüente – não há mais a necessidade de que eles sejam iguais, entretanto.

De maneira dual, temos que a regra $\wedge L$ em **G3c** é equivalente[3] a $\wedge L1 + \wedge L2 + weakL + contL$.

A admissibilidade da regra estrutural $Weakening$ no sistema **G3c** pode ser demonstrada através dos lemas a seguir.

Lema 1 ***[LWR]*** *Se* $\Gamma \vdash \Delta$ *é provável em* **G3c** *então* $\Gamma \vdash \Delta, C$ *é provável em* **G3c***.*

Prova Seja π prova de $\Gamma \vdash \Delta$ em **G3c**. A demonstração segue por indução no tamanho da prova π. Denote por ρ a última regra aplicada, assim temos:

- caso base ρ = axioma inicial

  $$\dfrac{}{\Gamma \vdash \Delta}\,inicial$$

  Logo temos que existe $A \in \Gamma, \Delta$. Sejam $\Gamma^1 = \Gamma - A$ e $\Delta^1 = \Delta - A$ Portanto, podemos concluir que

  Text $$\dfrac{}{\Gamma^1, A \vdash \Delta^1, A, C}\,inicial$$

  é uma prova de $\Gamma \vdash \Delta, C$

[3] No sentido de que **G3c** com a regra $\wedge R$ prova exatamente as mesmas fórmulas lógicas de **G** com as regras $\wedge R1$ e $\wedge R2$.

- caso $\rho = \wedge R$

$$\dfrac{\Gamma \vdash \Delta, A \quad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B} \wedge R$$

Pela hipótese de indução, existem π_1 prova de $\Gamma \vdash \Delta, A, C$ e π_2 prova de
$\Gamma \vdash \Delta, B, C$. Assim,

$$\dfrac{\overset{\pi_1}{\Gamma \vdash \Delta, A, C} \quad \overset{\pi_2}{\Gamma \vdash \Delta, B, C}}{\Gamma \vdash, A \wedge B, C} \wedge R$$

- caso $\rho = \supset R$

$$\dfrac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \supset B, \Delta} \supset R$$

Assim, pela hipótese de indução, existe π_1 prova de $\Gamma, A \vdash B, \Delta, C$. Logo,

$$\dfrac{\overset{\pi_1}{\Gamma, A \vdash B, \Delta, C}}{\Gamma \vdash A \supset B, \Delta, C} \supset R$$

- caso $\rho = \vee R$

$$\dfrac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee R$$

Pela hipótese de indução existe uma prova π_1 de $\Gamma \vdash A, B, \Delta, C$. Portanto,

$$\dfrac{\overset{\pi_1}{\Gamma \vdash A, B, \Delta, C}}{\Gamma \vdash A \vee B, \Delta, C} \vee R$$

- caso $\rho = \wedge L$

$$\dfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge L$$

Aplicando a hipótese de indução existe π_1 prova de $\Gamma, A, B \vdash \Delta, C$. Logo,

$$\dfrac{\overset{\pi_1}{\Gamma, A, B \vdash \Delta, C}}{\Gamma, A \wedge B \vdash \Delta, C} \wedge L$$

- caso $\rho = \vee L$

$$\dfrac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta} \vee L$$

Pela hipótese de indução, existem π_1 prova de $\Gamma, A \vdash \Delta, C$ e prova π_2 de $\Gamma, B \vdash \Delta, C$. Portanto,

$$\dfrac{\overset{\pi_1}{\Gamma, A \vdash \Delta, C} \quad \overset{\pi_2}{\Gamma, B \vdash \Delta, C}}{\Gamma, A \vee B \vdash \Delta, C} \vee L$$

- caso $\rho = \supset L$

$$\dfrac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \supset B \vdash \Delta} \supset L$$

Pela hipótese de indução, existem prova π_1 de $\Gamma \vdash A, \Delta, C$ e prova π_2 de $\Gamma, B \vdash \Delta, C$. Portanto,

$$\dfrac{\overset{\pi_1}{\Gamma \vdash A, \Delta, C} \quad \overset{\pi_2}{\Gamma, B \vdash \Delta, C}}{\Gamma, A \supset B \vdash \Delta, C} \supset L$$

Assim, podemos concluir [4] a demonstração. ∎

Este lema prova a admissibilidade da regra *weakR* em **G3c**. E de maneira inteiramente análoga podemos demonstrar que:

Lema 2 ***[LWL]****Se* $\Gamma \vdash \Delta$ *é provável em* **G3c** *então* $\Gamma, C \vdash \Delta$ *é provável em* **G3c***.*

Ou seja, a regra *weakL* também é admissível em **G3c**. Com isto, podemos afirmar que *Weakening* é admissível em **G3c**.

Definição 7 *Na conclusão de cada regra de inferência, a fórmula que não está em um contexto* (Γ *e* Δ) *é chamada* ***principal****.*

Para menções futuras à ultilização destes lemas, iremos denotá-los como **LWR** para o lema da admissibilidade da regra *weakR* e **LWL** para o lema da admissibilidade do *weakL* em **G3c**.

No sistema **G3c** a regra estrutural *Contraction* também é admissível. Primeiramente apresentaremos um lema conhecido como *lema da inversão*, necessário para a prova da admissibilidade do *contraction*.

[4]Omitimos os casos com os conectivos lógicos $\forall$ e $\exists$ nesta e nas demais demonstrações presentes nesta dissertação, por não fazerem parte de nossos estudos.

Lema 3 ***(Lema da inversão)***

1. *Se* $A \wedge B, \Gamma \vdash C$*, então* $A, B, \Gamma \vdash C$*;*

2. *Se* $A \vee B, \Gamma \vdash C$*, então* $A, \Gamma \vdash C$ *e* $B, \Gamma \vdash C$*;*

3. *Se* $A \supset B, \Gamma \vdash C$*, então* $\Gamma \vdash A, C$ *e* $B, \Gamma \vdash C$*.*

Prova

1. Se $A, \Gamma \vdash C$ é um axioma ou uma conclusão de $\bot L$; então, $A \wedge B$ não sendo atômico ou $\bot$, teremos também que $A, B, \Gamma \vdash C$ é um axioma ou conclusão de $\bot L$.
   Assumindo que a inversão é preservada até uma altura de derivação n. Seja $A \wedge B, \Gamma \vdash C$ de altura $n + 1$.
   Se $A \wedge B$ é a fórmula principal, a premissa $A, B, \Gamma \vdash C$ tem uma derivação de altura n.
   Se $A \wedge B$ não é principal na ultima regra, ele possui uma ou duas premissas $A \wedge B, \Gamma' \vdash C'$, $A \wedge B, \Gamma'' \vdash C''$, com derivação de altura $\leq n$. Então pela hitótese de indução, $A, B, \Gamma' \vdash C'$ e $A, B, \Gamma'' \vdash C''$. Agora aplicando a ultima regra nestas premissas podemos concluir em no máximo $n + 1$ passos que $A, B, \Gamma \vdash C$.

2. Como em (1), se $A \vee B, \Gamma \vdash C$ é um axioma, também $A, \Gamma \vdash C$ e $B, \Gamma \vdash C$ são axiomas.
   Se $A \vee B$ é a fórmula principal , as duas premissas $A, \Gamma \vdash C$ e $B, \Gamma \vdash C$ são deriváveis em n passos.
   Se $A \vee B$ não é uma fórmula principal na ultima regra, ela tem uma ou duas premissas $A \vee B, \Gamma' \vdash C'$, $A \vee B, \Gamma'' \vdash C''$ com derivação de altura $\leq n$. Portanto, pela hipótese de indução, $A, \Gamma' \vdash C'$ e $B, \Gamma' \vdash C'$ e $A, \Gamma'' \vdash C''$ e $B, \Gamma'' \vdash C''$.
   Agora, aplicando a ultima regra
   em $A, \Gamma' \vdash C'$ e $A, \Gamma'' \vdash C''$, concluímos que $A, \Gamma \vdash C$ e
   em $B, \Gamma' \vdash C'$ e $B, \Gamma'' \vdash C''$, concluímos que $B, \Gamma \vdash C$
   com no máximo $n + 1$ passos.

3. Para o caso em que $A \supset B, \Gamma \vdash C$ é um axioma, seguimos a ideia mostrada nos itens anteriores.
   Agora se $A \supset B$ é a fórmula principal, as premissas $\Gamma \vdash A, C$ e $B, \Gamma \vdash C$ tem derivações de altura n.
   Se $A \supset B$ não é principal na última regra, ela possui uma ou duas premissas $A \supset B, \Gamma' \vdash C'$ e $A \supset B, \Gamma'' \vdash C''$, com derivação de altura

$\leq n$.
Logo, por indução temos que $\Gamma' \vdash A, C'$ e $B, \Gamma' \vdash C'$ e $\Gamma'' \vdash A, C''$ e $B, \Gamma'' \vdash C''$. Aplicando a ultima regra em até $n+1$ passos
em $\Gamma' \vdash A, C'$ e $\Gamma'' \vdash A, C''$, concluimos que $\Gamma \vdash A, C$ e
em $B, \Gamma' \vdash C'$ e $B, \Gamma'' \vdash C''$, concluimos que $B, \Gamma \vdash C$.

∎

Lema 4 *Se $C, C, \Gamma \vdash \Delta$ é provável, então $C, \Gamma \vdash \Delta$ também é provável em* **G3c**.

Prova A prova será realizada por indução na altura de derivação n. Portanto, suponha que $C, C, \Gamma \vdash \Delta$ possui uma prova Π de altura n.

- **(Caso Base)** Se $n = 0$.
  $C, C, \Gamma \vdash \Delta$ é um axioma ou uma conclusão de $L\bot$ e portanto, Δ é um átomo no antecedente ou o antecedente contém $\bot$. Em ambos os casos, temos que $C, \Gamma \vdash \Delta$ é um axioma ou conclusão de $L\bot$.

Suponha que os resultados sejam verdadeiros para derivações de altura n. Seja $C, C, \Gamma \vdash \Delta$ com derivação de altura $n+1$. Temos dois casos possíveis: se a fórmula C não é principal ou é principal no último passo da inferência.

- Se a fórmula **C não é principal** na última regra aplicada, ela possui uma ou duas premissas $C, C, \Gamma' \vdash \Delta'$ e $C, C, \Gamma'' \vdash \Delta''$. (Seguiremos apenas com um premissa no texto, pois caso exista uma segunda premissa a prova desta é igual a que apresentaremos).

$$\frac{C, C, \Gamma' \vdash \Delta'}{C, C, \Gamma \vdash \Delta}$$

  então $C, C, \Gamma' \vdash \Delta'$ possui uma altura de derivação $\leq n$, pela hipótese de indução temos $C, \Gamma^{'} \vdash \Delta^{'}$ e aplicando-se a útima regra em até $n+1$ passos, $C, \Gamma \vdash \Delta$ é provável em G3c.

- Se **C é principal** na última regra, encontramos três casos de acordo com a forma de C:

  i $\wedge L$, $C = A \wedge B$, ou seja,

$$\frac{A, B, A \wedge B, \Gamma \vdash \Delta}{A \wedge B, A \wedge B, \Gamma \vdash \Delta} \wedge L$$

Então $A, B, A \wedge B, \Gamma \vdash \Delta$ tem derivação de altura n. Pelo primeiro item do lema (3) podemos afirmar que

$$A, B, A, B, \Gamma \vdash \Delta$$

pela hipótese de indução temos

$$A, B, B, \Gamma \vdash \Delta.$$

Novamente, pela hipótese de indução temos

$$A, B, \Gamma \vdash \Delta.$$

logo,

$$\frac{A, B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} \wedge L$$

e podemos concluir que $A \wedge B, \Gamma \vdash \Delta$ também é provável em **G3c**.

ii $\vee L$, $C = A \vee B$, ou seja,

$$\frac{\overset{\Pi_1}{A, A \vee B, \Gamma \vdash \Delta} \quad \overset{\Pi_2}{B, A \vee B, \Gamma \vdash \Delta}}{A \vee B, A \vee B, \Gamma \vdash \Delta} \vee L$$

Pelo item 2 do lema (3) temos que sendo Π_1 e Π_2 prováveis então

$$\overset{\Pi_{11}}{A, A, \Gamma \vdash \Delta} \text{ e } A, B, \Gamma \vdash \Delta$$
$$B, A, \Gamma \vdash \Delta \text{ e } \overset{\Pi_{22}}{B, B, \Gamma \vdash \Delta}$$

aplicado a hipótese de indução em Π_{11} e Π_{22}, temos que:

$$A, \Gamma \vdash \Delta \qquad B, \Gamma \vdash \Delta$$

e portanto,

$$\frac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \vee B, \Gamma \vdash \Delta} \vee L$$

ou seja, $A \vee B, \Gamma \vdash \Delta$ é provável.

iii $\supset L$, $C = A \supset B$, portanto,

$$\frac{A \supset B, \Gamma \vdash A, \Delta \quad A \supset B, \Gamma, B \vdash \Delta}{A \supset B, A \supset B, \Gamma \vdash \Delta} \supset L$$

é provável. Pelo terceiro item do lema 3 temos

$$\begin{array}{c} \Pi_1 \\ \Gamma \vdash A, A, \Delta \text{ e } \Gamma, B \vdash A, \Delta \end{array}$$

$$\begin{array}{c} \Pi_2 \\ \Gamma, B \vdash A, \Delta \text{ e } \Gamma, B, B \vdash \Delta \end{array}$$

pela hipótese de indução, em Π_1 e Π_2, temos

$$\Gamma \vdash A, \Delta \text{ e } \Gamma, B \vdash \Delta$$

assim,

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{A \supset B, \Gamma \vdash \Delta} \supset L$$

Com isto, podemos concluir a demonstração. ∎

Juntamente com o lema a seguir podemos concluir que a regra estrutural *Contration* é admissível em G3c.

Lema 5 *Se* $\Gamma \vdash \Delta, C, C$ *for provável em* **G3c** *então* $\Gamma \vdash \Delta, C$ *também será.*

Prova
A demonstração deste lema segue o mesmo raciocínio da prova do lema anterior, sendo assim, iremos omití-la neste texto. ∎

Como os contextos são todos copiados em **G3c**, o seguinte resultado pode ser facilmente provado:

Proposição 6 *O sistema* **G***, sem a regra CUT, é equivalente ao sistema* **G3c**.

Prova
Para demonstrarmos esta afirmação veremos, caso a caso, que toda regra pode ser simulada pelo outro sistema lógico. Afim de diferenciar as regras de cada sistema, iremos adcionar o índice G3c em todas as regras deste sistema e manteremos sem índice as regras do sistema G.

- Regra $\wedge$(conjunção) à direita
  Temos que $\wedge R \equiv \wedge R_{G3c} + LWR + LWL$.

$$\frac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash A \wedge B, \Delta_1, \Delta_2} \wedge R$$

$$\frac{\dfrac{\dfrac{\Gamma_1 \vdash A, \Delta_1}{\Gamma_1, \Gamma_2 \vdash A, \Delta_1} LWL}{\Gamma_1, \Gamma_2 \vdash A, \Delta_1, \Delta_2} LWR \quad \dfrac{\dfrac{\Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash B, \Delta_2} LWL}{\Gamma_1, \Gamma_2 \vdash B, \Delta_1, \Delta_2} LWR}{\Gamma_1, \Gamma_2 \vdash A \wedge B, \Delta_1, \Delta_2} \wedge R_{G3c}$$

e que $\wedge R_{G3c} \equiv ContL + ContR + \wedge R$.

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\wedge R_{G3c} \qquad \cfrac{\cfrac{\cfrac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma, \Gamma \vdash A \wedge B, \Delta, \Delta}\wedge R}{\Gamma, \Gamma \vdash A \wedge B, \Delta}ContR}{\Gamma \vdash A \wedge B, \Delta}ContL$$

- Regra $\vee$(disjunção) à direita
  Vemos que $\vee R1 \equiv \vee R_{G3c} + LWR$ e $\vee R2 \equiv \vee R_{G3c} + LWL$

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \vee B, \Delta}\vee R1 \qquad \cfrac{\cfrac{\Gamma \vdash A, \Delta}{\Gamma \vdash A, B, \Delta}LRW}{\Gamma \vdash A \vee B, \Delta}\vee R_{G3c}$$

$$\frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \vee B, \Delta}\vee R2 \qquad \cfrac{\cfrac{\Gamma \vdash B, \Delta}{\Gamma \vdash A, B, \Delta}LRL}{\Gamma \vdash A \vee B, \Delta}\vee R_{G3c}$$

também temos que $\vee R_{G3c} \equiv \vee R2 + \vee R1 + contR$

$$\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\vee R_{G3c} \qquad \cfrac{\cfrac{\cfrac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A, A \vee B, \Delta}\vee R2}{\Gamma \vdash A \vee B, A \vee B, \Delta}\vee R1}{\Gamma \vdash A \vee B, \Delta}contR$$

- Regra $\wedge$(conjunção) à esquerda
  Vê-se que $\wedge L1 \equiv \wedge L_{G3c} + LWL$ e $\wedge L2 \equiv \wedge L_{G3c} + LWL$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\wedge L1 \qquad \cfrac{\cfrac{\Gamma, A \vdash \Delta}{\Gamma, A, B \vdash \Delta}LWL}{\Gamma, A \wedge B \vdash \Delta}\wedge L_{G3c}$$

$$\frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\wedge L2 \qquad \cfrac{\cfrac{\Gamma, B \vdash \Delta}{\Gamma, A, B \vdash \Delta}LWL}{\Gamma, A \wedge B \vdash \Delta}\wedge L_{G3c}$$

e $\wedge L_{G3c} \equiv contL + \wedge L1 + \wedge L2$

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\wedge L_{G3c} \qquad \cfrac{\cfrac{\cfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A, A \wedge B \vdash \Delta}\wedge L2}{\Gamma, A \wedge B, A \wedge B \vdash \Delta}\wedge L1}{\Gamma, A \wedge B \vdash \Delta}contL$$

- Regra $\vee$(disjunção) à esquerda
  Temos que $\vee L \equiv \vee L_{G3c} + LWR + LWL$

$$\dfrac{\Gamma_1, A \vdash \Delta 1 \quad \Gamma_2, B \vdash \Delta_2}{\Gamma_1, \Gamma_2, A \vee B \vdash \Delta_1, \Delta_2}\ \vee L$$

$$\dfrac{\dfrac{\dfrac{\Gamma_1, A \vdash \Delta_1}{\Gamma_1, \Gamma_2, A \vdash \Delta_1}\ LWL}{\Gamma_1, \Gamma_2, A \vdash \Delta_1, \Delta_2}\ LWR \quad \dfrac{\dfrac{\Gamma_2, B \vdash \Delta_2}{\Gamma_1, \Gamma_2, B \vdash \Delta_2}\ LWL}{\Gamma_1, \Gamma_2, B \vdash \Delta_1, \Delta_2}\ LWR}{\Gamma_1, \Gamma_2, A \vee B \vdash \Delta_1, \Delta_2}\ \vee L_{G3c}$$

e $\vee L_{G3c} \equiv contL + contR + \vee L$

$$\dfrac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ \vee L_{G3c} \qquad \dfrac{\dfrac{\dfrac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, \Gamma, A \vee B \vdash \Delta\Delta}\ \vee L}{\Gamma, \Gamma, A \vee B \vdash \Delta}\ contR}{\Gamma, A \vee B \vdash \Delta}\ contL$$

- Regra $\supset$(implicação) à esquerda
  Nota-se que $\supset L \equiv \supset L_{G3c} + LWR + LWL$

$$\dfrac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2, B \vdash \Delta_2}{\Gamma_1, \Gamma_2, A \supset B \vdash \Delta_1 \Delta_2}\ \supset L$$

$$\dfrac{\dfrac{\dfrac{\Gamma_1 \vdash A, \Delta_1}{\Gamma_1, \Gamma_2 \vdash A, \Delta_1}\ LWL}{\Gamma_1, \Gamma_2 \vdash A, \Delta_1 \Delta_2}\ LWR \quad \dfrac{\dfrac{\Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash B, \Delta_2}\ LWL}{\Gamma_1, \Gamma_2 \vdash B, \Delta_1 \Delta_2}\ LWR}{\Gamma_1, \Gamma_2, A \supset B \vdash \Delta_1 \Delta_2}\ \supset L_{G3c}$$

e $\supset L_{G3c} \equiv contL + contR + \supset L$

$$\dfrac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \supset B \vdash \Delta}\ \supset L_{G3c} \qquad \dfrac{\dfrac{\dfrac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, \Gamma, A \supset B \vdash \Delta, \Delta}\ \supset L}{\Gamma, \Gamma, A \supset B \vdash \Delta}\ contR}{\Gamma, A \supset B \vdash \Delta}\ contL$$

Pelas Figuras 4 e 5, podemos ver que as demais regras são iguais. Portanto, podemos concluir que os sistemas **G** e **G3c** são equivalentes. ∎

O sistema **G3c** é computacionalmente mais interessante que **G** uma vez que, como as regras estruturais *weak* e *cont* são *implícitas*, ele pode ser facilmente implementado.

3.2 Cut elimination - A eliminação da regra de Corte

Agora provaremos que a regra *Cut* pode ser eliminada do sistema **G**. Desta forma, **G** e **G3c** são equivalentes.

Talvez a regra lógica mais conhecida em cálculo de seqüentes seja a regra *Cut*:

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad A, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ (Cut)$$

Basicamente, essa regra formaliza o conceito de provas matemáticas utilizando lemas auxiliares. Ou seja, se podemos provar um lema A (e outros resultados Δ_1) a partir de um conjunto de hipóteses Γ_1 e, a partir de A (e possivelmente algumas outras hipóteses Γ_2) é possível provar outro conjunto de resultados (Δ_2), então podemos provar Δ_1, Δ_2 diretamente a partir de Γ_1, Γ_2.

Essa ideia é utilizada sempre em Matemática mas é também muito interessante sob o ponto de vista computacional, uma vez que a implementação de tal regra é feita "*bottom-up*". Ou seja, para tentar provar Δ_1, Δ_2 a partir de Γ_1, Γ_2, primeiro tentamos provar uma fórmula A (para uma certa fórmula desconhecida A), e a partir de A tentamos provar Δ_2. Isto significa que a fórmula lógica A deve ser "adivinhada" pelo programa de computador e isso representa um problema muito sério, uma vez que computadores não tem a "criatividade" necessária para adivinhar fórmulas.

Portanto, é muito importante dentro da área de programação lógica a possibilidade de se verificar se um sistema lógico possui a propriedade de *cut-elimination*, ou seja, checar se a regra *Cut* é, de fato, redundante e portanto pode ser eliminada.

Enquanto para Ciência da Computação a importância da propriedade de *cut-elimination* está relacionada com a viabilidade de implementações, para os matemáticos essa propriedade reforça o fato de que lemas são ferramentas úteis para organizar uma prova, mas completamente dispensáveis. Ou seja, toda prova que utiliza a regra *Cut* pode ser substituída por uma onde *Cut* não está presente.

Checar se um sistema lógico possui a propriedade de *cut-elimination* é, em geral, um problema não trivial (veja, por exemplo, [18, 19, 24]).

Teorema 7 *A regra* Cut *pode ser eliminada no sistema lógico* **G***, ou seja, o sistema possui a propriedade* cut-elimination.

Prova A prova de que a regra *Cut* pode ser eliminada do sistema **G** é feita através do método de exaustão aliado à indução estrutural. De maneira mais clara, tomamos como base a prova Π do seqüente $\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$:

$$\dfrac{\begin{array}{c}\Pi_1\\ \Gamma_1 \vdash \Delta_1, A\end{array} \quad \begin{array}{c}\Pi_2\\ A, \Gamma_2 \vdash \Delta_2\end{array}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ Cut$$

tal que esta seja a aplicação da regra *Cut* mais perto das folhas[5]. Desta forma, Π_1 e Π_2 não possuem aplicações da regra *Cut* – são *livres de cut*. Olhamos agora para a última regra aplicada em Π_1 e Π_2:

Separaremos esta demonstração em dois casos principais. O primeiro caso, ocorre quando pelo menos uma premissa na regra *Cut* é um axioma ou uma conclusão de $\bot L$. E o segundo, quando nenhuma das premissas são axiomas.

Caso i Admitimos a regra *Cut* com um axioma ou conclusão $\bot L$ como premissa. Se pelo menos uma premissa de *Cut* é um axioma, nos podemos separar o caso em dois: na premissa da esquerda ou na premissa da direita.

i.1 *Na premissa da esquerda*

i.1.1 Na premissa da esquerda Π_1, temos que $A \in \Gamma_1$. Neste caso podemos obter $\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$ de $A, \Gamma_2 \vdash \Delta_2$ por *Weakening*.

$$\dfrac{\dfrac{}{\Gamma_1', A \vdash \Delta_1, A}\ inicial \qquad A, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ cut \Longrightarrow \dfrac{\dfrac{A, \Gamma_2 \vdash \Delta_2}{\Gamma_1', A, \Gamma_2 \vdash \Delta_2}\ weakL}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ weakR$$

onde $\Gamma_1' = \Gamma_1 - A$.

i.1.2 $\bot$ é uma fórmula em Γ_1 , onde $\Gamma_1' = \Gamma_1 - \bot$

$$\dfrac{\dfrac{}{\bot, \Gamma_1' \vdash \Delta_1, A}\ L\bot \qquad A, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ cut$$

Então $\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$ é uma conclusão de $L\bot$, pois $\bot \in \Gamma_1$.

i.2 *Na premissa da direita*

i.2.1 Na premissa da direita, $\Delta_2 \in \Gamma_2$, onde $\Gamma_2' = \Gamma_2 - \Delta_2$

$$\dfrac{\Gamma_1 \vdash \Delta_1, A \qquad \dfrac{}{A, \Delta_2, \Gamma_2' \vdash \Delta_2}\ inicial}{\Gamma_1, \Gamma_2', \Delta_2 \vdash \Delta_1, \Delta_2}\ Cut$$

Então $\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$ é um axioma.

[5]Existe um jeito formal de definir o que é *mais perto* através o conceito de altura de provas.

i.2.2 Na premissa da direita $\Delta_2 = A$.

$$\dfrac{\Gamma_1 \vdash \Delta_1, A \quad \dfrac{}{A, \Gamma_2 \vdash A}\,inicial}{\Gamma_1, \Gamma_2 \vdash \Delta_1, A}\,Cut$$

Então sendo $\Delta_2 = A$ a primeira premissa é $\Gamma_1 \vdash \Delta_1, \Delta_2$. E $\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$ segue por *Weakening*.

$$\dfrac{\Gamma_1 \vdash \Delta_1, \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,weakR$$

i..2.3 $\perp \in \Gamma_2$

$$\dfrac{\Gamma_1 \vdash \Delta_1, A \quad \dfrac{}{A, \perp\Gamma_1' \vdash \Delta_2}\,L\perp}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,Cut$$

Como $\perp \in \Gamma_2$ concluímos que $\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$ é uma conclusão de $L\perp$.

i.2.4 $A = \perp$

$$\dfrac{\Gamma_1 \vdash \Delta_1, \perp \quad \perp, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,cut$$

Então a primeira premissa $\Gamma_1 \vdash \Delta_1, \perp$ é um axioma e $\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2$ segue como no caso (i.1). Ou, $\Gamma_1 \vdash \Delta_1, \perp$ foi obtido por uma regra à esquerda. E portanto, as transformações são casos especiais com $\Delta = \perp$, dos três casos apresentados a seguir.

Caso ii Assumindo *Cut* com nenhuma premissa como axioma. Assim, temos portanto, três possibilidades: Quando a fórmula *cut* não é principal em nenhuma premissa do *Cut*, quando a fórmula *cut* é principal em apenas uma premissa e quando ela é principal em ambas premissas do *Cut*.

ii.1 A fórmula cut **C não é principal** na premissa da *esquerda* (prova análoga no caso à direita), isto é, não deriva de uma R-regra (L-regra).

ii.1.1 $\wedge L$, com $\Gamma_1 = A \wedge B, \Gamma_1'$

$$\dfrac{\dfrac{B, \Gamma_1' \vdash \Delta_1, C}{A \wedge B, \Gamma_1' \vdash \Delta_1, C}\,\wedge L2 \quad C, \Gamma_2 \vdash \Delta_2}{A \wedge B, \Gamma_1', \Gamma_2 \vdash \Delta_1, \Delta_2}\,cut$$

que pode ser transformado por permutação de ordem $\wedge L2, Cut$ em $Cut, \wedge L2$.

$$\dfrac{\dfrac{B, \Gamma_1' \vdash \Delta_1, C \quad C, \Gamma_2 \vdash \Delta_2}{B, \Gamma_1', \Gamma_2 \vdash \Delta_1, \Delta_2}\,Cut}{A \wedge B, \Gamma_1', \Gamma_2 \vdash \Delta_1, \Delta_2}\,\wedge L2$$

O mesmo ocorre quando usamos a regra $\wedge L1$.

ii.1.2 $\lor L$, onde $\Gamma_1 = A \lor B, \Gamma'_1$, $\Gamma'_1 = \Gamma''_1 \cup \Gamma'''_1$, $\Delta'_1 = \Delta''_1 \cup \Delta'''_1$ e $C = C'' \cup C'''$.

$$\dfrac{\dfrac{\overset{\pi_1}{\Gamma''_1, A \vdash \Delta''_1, C''} \qquad \overset{\pi_2}{\Gamma'''_1, B \vdash \Delta'''_1, C'''}}{A \lor B, \Gamma'_1 \vdash \Delta_1, C}\,\lor L \qquad \overset{\pi_3}{C, \Gamma_2 \vdash \Delta_2}}{A \lor B, \Gamma'_1, \Gamma_2 \vdash \Delta_1 \Delta_2}\,Cut$$

transformamos em

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overset{\pi_1}{\Gamma''_1, A \vdash \Delta''_1, C''}}{\Gamma''_1, A \vdash \Delta''_1, C}\,\mathit{weakR} \qquad \overset{\pi_3}{C, \Gamma_2 \vdash \Delta_2}}{A, \Gamma''_1, \Gamma_2 \vdash \Delta''_1, \Delta_2}\,\mathit{cut} \qquad \dfrac{\dfrac{\overset{\pi_2}{\Gamma'''_1, B \vdash \Delta'''_1, C'''}}{\Gamma'''_1, B \vdash \Delta'''_1, C}\,\mathit{weakR} \qquad \overset{\pi_3}{C, \Gamma_2 \vdash \Delta_2}}{B, \Gamma'''_1, \Gamma_2 \vdash \Delta'''_1, \Delta_2}\,\mathit{cut}}{A \lor B, \Gamma'_1, \Gamma_2, \Gamma_2 \vdash \Delta_1, \Delta_2, \Delta_2}\,\lor L}{A \lor B, \Gamma'_1, \Gamma_2, \Gamma_2 \vdash \Delta_1, \Delta_2}\,\mathit{contR}}{A \lor B, \Gamma'_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,\mathit{contL}$$

ii.1.3 $\supset L$, com $\Gamma_1 = A \supset B, \Gamma'_1$.

$$\dfrac{\dfrac{\overset{\pi_1}{\Gamma''_1 \vdash A, \Delta''_1, C''} \qquad \overset{\pi_2}{\Gamma'''_1, B \vdash \Delta'''_1, C'''}}{A \supset B, \Gamma'_1 \vdash \Delta_1, C}\,\supset L \qquad \overset{\pi_3}{C, \Gamma_2 \vdash \Delta_2}}{A \supset B, \Gamma'_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,\mathit{cut}$$

que pode ser reordenado da seguinte maneira,

$$\dfrac{\dfrac{\dfrac{\overset{\pi_1}{\Gamma''_1 \vdash A, \Delta''_1, C''}}{\Gamma''_1 \vdash A, \Delta''_1, C}\,\mathit{weakR} \qquad \overset{\pi_3}{C, \Gamma_2 \vdash \Delta_2}}{\Gamma''_1, \Gamma_2 \vdash A, \Delta''_1, \Delta_2}\,\mathit{cut} \qquad \dfrac{\dfrac{\overset{\pi_2}{\Gamma'''_1, B \vdash \Delta'''_1, C'''}}{\Gamma'''_1, B \vdash \Delta'''_1, C}\,\mathit{weakR} \qquad \overset{\pi_3}{C, \Gamma_2 \vdash \Delta_2}}{\Gamma'''_1, B, \Gamma_2 \vdash \Delta'''_1, \Delta_2}\,\mathit{cut}}{A \supset B, \Gamma'_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,\supset L$$

ii.1.4 $\land R$, onde $\Delta_1 = A \land B$.

$$\dfrac{\dfrac{\overset{\pi_1}{\Gamma'_1 \vdash A, C'} \qquad \overset{\pi_2}{\Gamma''_1 \vdash B, C''}}{\Gamma_1 \vdash A \land B, C}\,\land R \qquad \overset{\pi_3}{C, \Gamma_2 \vdash \Delta_2}}{\Gamma_1, \Gamma_2 \vdash A \supset B, \Delta_2}\,\mathit{cut}$$

que pode ser transformado em,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overset{\pi_1}{\Gamma'_1 \vdash A, C'}}{\Gamma'_1 \vdash A, C}\,\mathit{weakR} \qquad \overset{\pi_3}{C, \Gamma_2 \vdash \Delta_2}}{\Gamma'_1, \Gamma_2 \vdash A, \Delta_2}\,\mathit{cut} \qquad \dfrac{\dfrac{\overset{\pi_2}{\Gamma''_1 \vdash B, C''}}{\Gamma''_1 \vdash B, C}\,\mathit{weakR} \qquad \overset{\pi_3}{C, \Gamma_2 \vdash \Delta_2}}{\Gamma''_1, \Gamma_2 \vdash B, \Delta_2}\,\mathit{cut}}{\Gamma_1, \Gamma_2, \Gamma_2 \vdash A \land B, \Delta_2, \Delta_2}\,\land R}{\Gamma_1, \Gamma_2, \Gamma_2 \vdash A \land B, \Delta_2}\,\mathit{contR}}{\Gamma_1, \Gamma_2 \vdash A \land B, \Delta_2}\,\mathit{contL}$$

ii.1.5 $\vee R$, com $\Delta_1 = A \vee B$

$$\dfrac{\dfrac{\overset{\pi_1}{\Gamma_1 \vdash A, C}}{\Gamma_1 \vdash A \vee B, C}\,\vee R1 \qquad \overset{\pi_2}{C, \Gamma_2 \vdash \Delta_2}}{\Gamma_1, \Gamma_2 \vdash A \vee B, \Delta_2}\,cut$$

reordenado

$$\dfrac{\dfrac{\overset{\pi_1}{\Gamma_1 \vdash A, C} \quad \overset{\pi_2}{C, \Gamma_2 \vdash \Delta_2}}{\Gamma_1, \Gamma_2 \vdash A, \Delta_2}\,cut}{\Gamma_1, \Gamma_2 \vdash A \vee B, \Delta_2}\,\vee R1$$

Caso Dual para regra $\vee R2$.

ii.1.6 $\supset R$, onde $\Delta_1 = A \supset B$.

$$\dfrac{\dfrac{\overset{\pi_1}{\Gamma_1, A \vdash B, C}}{\Gamma_1 \vdash A \supset B, C}\,\supset R \qquad \overset{\pi_2}{C, \Gamma_2 \vdash \Delta_2}}{\Gamma_1, \Gamma_2 \vdash A \supset B, \Delta_2}\,cut$$

transformado em,

$$\dfrac{\dfrac{\overset{\pi_1}{\Gamma_1, A \vdash B, C} \quad \overset{\pi_2}{C, \Gamma_2 \vdash \Delta_2}}{\Gamma_1, \Gamma_2, A \vdash B, \Delta_2}\,cut}{\Gamma_1, \Gamma_2 \vdash A \supset B, \Delta_2}\,\supset R$$

Podemos notar que em cada um dos subcasos apresentados, a altura da regra *Cut* foi reduzida após a transformação.

ii.2 A fórmula cut **C é principal** apenas na premissa da esquerda (direita).

Omitiremos aqui a demonstração deste caso, pois ela é análoga ao caso que acabamos de apresentar.

ii.3 A fórmula cut **C é principal em ambas** premissas.

ii.3.1 $C = A \wedge B$.

$$\dfrac{\dfrac{\overset{\pi_1}{\Gamma_1' \vdash \Delta_1', A} \quad \overset{\pi_2}{\Gamma_1'' \vdash \Delta_1'', B}}{\Gamma_1 \vdash \Delta_1, A \wedge B}\,\wedge R \qquad \dfrac{\overset{\pi_3}{A, \Gamma_2 \vdash \Delta_2}}{A \wedge B, \Gamma_2 \vdash \Delta_2}\,\wedge L2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,cut$$

é reordenado

$$\dfrac{\dfrac{\dfrac{\overset{\pi_1}{\Gamma_1' \vdash \Delta_1', A}}{\Gamma_1 \vdash \Delta_1', A}\,\mathit{weakL}}{\Gamma_1 \vdash \Delta_1, A}\,\mathit{weakR} \qquad \overset{\pi_3}{A, \Gamma_2 \vdash \Delta_2}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,\mathit{cut}$$

ii.3.2 $C = A \vee B$.

$$\dfrac{\dfrac{\overset{\pi_1}{\Gamma_1 \vdash \Delta_1, A}}{\Gamma_1 \vdash \Delta_1, A \vee B}\,\vee R1 \qquad \dfrac{\overset{\pi_2}{A, \Gamma_2' \vdash \Delta_2'} \quad \overset{\pi_3}{B, \Gamma_2'' \vdash \Delta_2''}}{A \vee B \Gamma_2 \vdash \Delta_2}\,\vee L}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,\mathit{cut}$$

transformamos em,

$$\dfrac{\overset{\pi_1}{\Gamma_1 \vdash \Delta_1, A} \qquad \dfrac{\dfrac{\overset{\pi_2}{A, \Gamma_2' \vdash \Delta_2'}}{A, \Gamma_2 \vdash \Delta_2'}\,\mathit{weakL}}{A, \Gamma_2 \Delta_2}\,\mathit{weakR}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,\mathit{cut}$$

ii.3.3 $C = A \supset B$.

$$\dfrac{\dfrac{\overset{\pi_1}{\Gamma_1, A \vdash B, \Delta_1}}{\Gamma_1 \vdash \Delta - 1, A \supset B}\supset R \qquad \dfrac{\overset{\pi_2}{\Gamma_2' \vdash A, \Delta_2'} \quad \overset{\pi_3}{B, \Gamma_2'' \vdash \Delta_2''}}{A \supset B, \Gamma_2 \vdash \Delta_2}\supset L}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,\mathit{cut}$$

é transformado em,

$$\dfrac{\dfrac{\overset{\pi_2}{\Gamma_2' \vdash A, \Delta_2'} \quad \overset{\pi_1}{\Gamma_1, A \vdash B, \Delta_1}}{\Gamma_1, \Gamma_2' \vdash B, \Delta_1, \Delta_2'}\,\mathit{cut} \qquad \overset{\pi_3}{B, \Gamma_2'' \vdash \Delta_2''}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,\mathit{cut}$$

Note que em cada subcaso o *Cut* foi simplificado após a transformação. Desta forma, podemos eliminar os cortes que aparecem nas folhas da prova e substituímos cortes internos por cortes mais simples ou mais perto das folhas. Ou seja, sobram eventualmente apenas cortes sobre átomos, que são novamente movidos na direção das folhas e então eliminados. ∎

Vale observar que, como uma primeira conseqüência imediata da propriedade de *cut-elimination*, as lógicas clássica e intuicionista de primeira ordem são **consistentes**. De fato, é fácil ver que não há prova possível para $\perp(falso)$: as únicas regras de inferência que poderiam ser usadas para provar o seqüente (que não a regra *Cut*)

$$\vdash \perp$$

seriam *contr R* e *weak R* e essas regras, isoladamente, não levam a uma prova.

Uma segunda conseqüencia interessante é que todos os seqüentes que ocorrem na prova de um sequente $\Gamma \rightarrow \Delta$ onde a regra *Cut* não é utilizada contêm fórmulas que são sub-fórmulas de uma fórmula em Γ ou em Δ. Isso é chamado de propriedade da *sub-fórmula*.

Finalmente, apesar de que os cortes podem ser eliminados de provas, existem poucos seqüentes matemáticos interesantes que possuam provas livres do uso da regra *Cut* que podem ser escritos ou armazenados na memória de um computador.

3.3 Especificando a lógica clássica

Para especificar um seqüente, devemos primeiro descrever um predicado que diz respeito à *provabilidade* de um seqüente:

```
type prova     list form -> list form -> o.
```

Ou seja, `prova` é um predicado que toma listas de fórmulas Γ e Δ e traz como resultado se Γ segue de Δ ou não.

Depois, seguimos especificando o axioma inicial:

```
prova G H :- membro A G, membro A H.
```

Ou seja, se `A` aparece em ambos os lados do seqüente, a prova acaba. Aqui `membro` é um predicado definido em um outro módulo do programa que trata de listas (veja Apêndice A). Intuitivamente, `membro A G` retorna verdadeiro se o elemento `A` pertence à lista `G`.

Podemos então seguir especificando as outras regras do sistema:

```
prova G H :- membro true H.
prova G H :- memb_and_rest (A and B) H H1, prova G (A::H1),
             prova G (B::H1).
prova G H :- memb_and_rest (A imp B) H H1, prova (A::G) (B::H1).
prova G H :- memb_and_rest (neg A) H H1, prova (A::G) H1.
prova G H :- memb_and_rest (A or B) H H1, prova G (A::(B::H1)).
prova G H :- memb_and_rest (forall A) H H1,
```

```
             pi x\(prova G ((A x)::H1)).
prova G H :- memb (exists A) H, prova G ((A T)::H).

prova G H :- membro false G.
prova G H :- memb_and_rest (neg A) G G1, prova G1 (A::H).
prova G H :- memb_and_rest (A and B) G G1,
             prova (A ::(B :: G1)) H.
prova G H :- memb_and_rest (A or B) G G1, prova (A :: G1) H,
             prova (B :: G1) H.
prova G H :- memb_and_rest (A imp B) G G1, prova (B::G1) H,
             prova G1 (A::H).
prova G H :- memb (forall A) G, prova ((A T)::G) H.
prova G H :- memb_and_rest (exists A) G G1,
             pi x\(prova ((A x)::G1) H).
```

A especificação do predicado `memb_and_rest` é apresentada no Apêndice A. Intuitivamente, `memb_and_rest A G G1` retorna verdadeiro se `A` aparece em `G` e `G1` é `G-A`.

Apesar de termos apresentado a especificação de toda lógica clássica de primeira ordem, PLLIC lida apenas com a *parte proposicional* das lógicas implementadas, uma vez que é um provador de teoremas *completamente automático* e *decidível*. Mas é importante notar que pode-se estender PLLIC de modo que este torne-se indecidível mas suporte quantificação, ou mesmo semi-automático suportando, entre outras coisas, indução (veja por exemplo [24]).

3.4 Semântica

Quando identificamos fórmulas logicamente equivalentes no cálculo proposicional, obtemos um conjunto do qual, de maneira natural, podemos definir uma operação unitária e duas operações binárias que correspondem respectivamente a negação, conjunção (*operador* : $\cdot$) e disjunção (*operador* : $+$). A estrutura obtida desta maneira é uma álgebra booleana.

A álgebra booleana pode ser apresentada de maneiras distintas. Neste texto a apresentaremos de maneira puramente álgebrica (como anéis e como conjuntos ordenados) e também veremos que podemos adotar um ponto de vista topológico.

Considere, nesta e em seções futuras, o conjunto de variáveis proposicionais (denotado por P) e o conjunto correspondente $\mathcal{P}$ de fórmulas proposicionais.

Definiremos agora a aplicação valoração, para a lógica clássica e algumas propriedades importantes.

Uma valoração (ou atribuição de valores verdadeiros) δ para P é um elemento do conjunto $\{\mathbf{0,1}\}^P$. Ela atribui, para cada variável proposicional p de P, um valor $\delta(p)$ que é **0** ou **1** (intuitivamente, falso ou verdadeiro). Formalmente temos:

Definição 8 *Uma **valoração** para P é uma aplicação de P sobre o conjunto* $\{\boldsymbol{0,1}\}$.

Estenderemos agora a definição para todas as fórmulas da lógica clássica proposicional $\mathcal{P}$.

Definição 9 *Seja* $\mathcal{B} = \{0,1\}$. *Dada uma valoração* δ, *defina o aplicação* $[\![\bullet]\!]_\delta : \mathcal{P} \to \mathcal{B}$ *por:*

$$\begin{aligned} [\![p]\!]_\delta &= \delta(p),, \ \texttt{para } p \in P\texttt{;} \\ [\![\bot]\!]_\delta &= 0; \\ [\![\varphi \vee \psi]\!]_\delta &= max\,\{[\![\varphi]\!]_\delta, [\![\psi]\!]_\delta\} \\ [\![\varphi \wedge \psi]\!]_\delta &= min\,\{[\![\varphi]\!]_\delta, [\![\psi]\!]_\delta\} \\ [\![\varphi \to \psi]\!]_\delta &= max\,\{1 - [\![\varphi]\!]_\delta, [\![\psi]\!]_\delta\} \end{aligned} \tag{1}$$

Escreveremos $\overline{\delta}(\varphi)$ *no lugar de* $[\![\varphi]\!]_\delta$.

Lema 8 *Para qualquer fórmula $F\left[A_1, A_2, ..., A_n\right]$ e qualquer atribuição de valores verdadeiros λ e $\mu \in \{\boldsymbol{0,1}\}^P$, se λ e μ são iguais em $[A_1, A_2, ..., A_n]$, então $\bar{\lambda}(F) = \bar{\mu}(F)$.*

Definição 10
- *Uma **tautologia** é uma fórmula que assume o valor 1 para todas as valorações* possíveis.
- *A notação para 'F é uma tautologia' é: $\vdash^* F$.*
- *Dadas duas fórmulas F e G, F é **logicamente equivalente** a G ($F \sim G$) se e somente se a fórmula ($F \Leftrightarrow G$) é uma tautologia.*

A próximas duas propriedades seguem imediatamente das definições acima.

- Para todas as fórmulas F e G, temos que $F \sim G$ se e somente se para toda valoração $\delta \in \{0,1\}^P$, $\bar{\delta}(F) = \bar{\delta}(G)$.
- A relação binária $\sim$ é uma relação de equivalência em A

A valoração também possui as seguintes propriedades:

- $\bar{\delta}(\neg F) = 1 + \bar{\delta}(F)$.
- $\bar{\delta}(F \Leftrightarrow G) = 1 + \bar{\delta}(F) + \bar{\delta}(G)$.

Definição 11 *Sejam $\mathcal{A}$ e $\mathcal{B}$ subconjuntos de P, seja G uma fórmula e δ uma valoração para P.*

- *$\mathcal{A}$ é **satisfeito** por δ se e só se δ satisfaz todas as fórmulas de $\mathcal{A}$.*
- *$\mathcal{A}$ é **consistente** se e somente se existe pelo menos uma valoração que satisfaz $\mathcal{A}$.*
- *$\mathcal{A}$ é **finitamente satisfeito** se e somente se todo subconjunto finito de $\mathcal{A}$ é satisfeito.*
- *$\mathcal{A}$ é **contraditório** se e só se não é consistente.*
- *G é uma **consequência de** $\mathcal{A}$ (que denotamos por $\mathcal{A} \vdash^* G$) se e somente se toda valoração que satisfaz $\mathcal{A}$ satisfaz G.*
- *$\mathcal{A}$ e $\mathcal{B}$ são **equivalentes** se e somente se toda fórmula de $\mathcal{A}$ é uma consequência de $\mathcal{B}$ e toda fórmula de $\mathcal{B}$ é uma consequência de $\mathcal{A}$.*

Com as propriedades da valoração apresentadas acima construiremos uma tabela de valores, conhecida como **tabela da verdade**, para a negação, conjunção, disjunção, implicação e equivalência.

F	**¬ F**
0	1
1	0

F	**G**	$(F \wedge G)$
0	0	0
1	0	0
0	1	0
1	1	1

F	**G**	$(F \vee G)$
0	0	0
1	0	1
0	1	1
1	1	1

F	**G**	$(F \Rightarrow G)$
0	0	1
1	0	0
0	1	1
1	1	1

F	**G**	$(F \Leftrightarrow G)$
0	0	1
1	0	0
0	1	0
1	1	1

3.4.1 Topologia

Apresentaremos agora, algumas definições e resultados da topologia, necessários para uma melhor compreensão das arfimações feitas em seções posteriores.

Uma **topologia** para um conjunto X é uma família de subconjuntos $\mathcal{F}$ de X tais que o conjunto vazio e o conjunto X devem pertencer à topologia $\mathcal{F}$; a reunião arbitrária de elementos da topologia deve pertencer à topologia e a interseção finita de elementos da topologia deve pertencer à topologia. O par $(X, \mathcal{F})$ é chamado **espaço topológico**. Para facilitar a notação, escreveremos apenas X para o espaço topológico $(X, \mathcal{F})$.

Seja X um espaço topológico e Y um subconjunto de X. Damos a Y uma topologia, chamada **a topologia induzida em Y pela de X**, tomando como conjuntos abertos nesta topologia as interseções com Y dos subconjuntos abertos de X. Em outras palavras, para um subconjunto $\Omega \subseteq Y$ ser aberto em uma topologia induzida, é necessário e suficiente que exista um conjunto aberto O na topologia de X tal que $\Omega = O \cap Y$. Vemos imediatamente que os conjuntos fechados para uma topologia induzida em Y são as interseções dos subconjuntos fechados de X com Y. Um **subespaço** de um espaço topológico X é um subconjunto de X e sua topologia induzida.

A **base** de um conjunto aberto de um espaço topológico X é uma família $(O_i)_{i \in I}$ de conjuntos abertos na topologia, tal que, todo conjunto aberto é uma união de conjuntos abertos desta família; em outras palavras, para todo conjunto aberto G, há pelo menos um subconjunto $J \subseteq I$ tal que $G = \bigcup_{j \in J} O_j$. Quando a base dos conjuntos abertos de um espaço topológico é escolhida, os elementos desta base são chamados **conjuntos abertos básicos**. Os complementos em X dos conjuntos abertos básicos são chamados **conjuntos fechados básicos** e fica claro que todo conjunto fechado é uma interseção de conjuntos fechados básicos.

Definição 12 *Um espaço topológico X é **Hausdorff** se e somente se para todo par de elementos disjunto x e y de X existem conjuntos abertos disjuntos G e H tais que, $x \in G$ e $y \in H$. É imediato que todo subespaço de um espaço de Hausdorff é Hausdorff.*

Lema 9 *Seja X um espaço topológico que é Hausdorff e seja Y um subconjunto de X. Então a topologia induzida em Y de X faz de Y um espaço de Hausdorff.*

Prova
Se x e y são pontos distintos de Y, a interseção com Y de dois subconjuntos abertos disjuntos de X que contem x e y serão respectivamento dois subconjundos abertos disjuntos de Y que contem x e y respectivamente. ▮

Definição 13 *Uma **cobertura** de um espaço topológico X é uma família $(E_i)_{i \in I}$ de subconjuntos de X tal que $X = \bigcup_{i \in I} E_i$. Se todos os E_i são conjuntos abertos, dizemos que é uma **cobertura aberta**. Uma **subcobertura** de uma cobertura $(E_i)_{i \in I}$ é uma subfamília $(E_j)_{j \in J}$ $(J \subseteq I)$ que também cobre de X. Falamos de cobertura (ou subcobertura) **finita** quando o conjunto correspondente de índices é finito.*

Definição 14 *Um espaço topológico é chamado **compacto** se e somente se*

1. *É Hausdorff*
2. *De toda cobertura aberta de X podemos extrair uma subcobertura finita.*

Lema 10 *Seja X um espaço de Hausdorff. Para X ser compacto, é necessário e suficiente que toda família de subconjuntos fechados de X cuja interseção é não vazia tenha uma subfamília finita cuja interseção é não vazia.*

Prova
É suficiente observar que se $(F_i)_{i \in I}$ é uma família de subconjuntos fechados de X e se, para cada $i \in I$, denote o complemento de F_i em X por O_i (que é um conjunto aberto), então $\bigcap_{i \in I} F_i = \emptyset$ se e somente se $\bigcup_{i \in I} O_i = X$. Assim, cada família de subconjuntos fechados de X cuja interseção é vazia, corresponde, por complementação, a uma cobertura aberta de X, e vice-versa. ▮

Definição 15 *Um subconjunto de um espaço topológico X que é simultaneamente aberto e fechado (isto é, um subconjunto aberto cujo complemento também é aberto) será chamado de **aberto-fechado**.*

Definição 16 *Um espaço topológico que tem uma base formada por conjuntos abertos-fechados é chamado **zero-dimensional**.*

Lema 11 *Para um espaço topológico ser zero-dimensional, é necessário e suficiente que a família de subconjuntos abertos-fechados seja uma base para os conjuntos abertos.*

Prova

Text

E fácil ver que qualquer família de conjuntos abertos que inclui uma base para os subconjuntos abertos de X é, ela mesma, uma base para os subconjuntos de X. Assim, se X é zero-dimensional, então a família de todos os subconjuntos abertos-fechados é uma base para os conjuntos abertos. O inverso é imediato. Ou seja, se a base para os conjuntos abertos é formada por subconjuntos abertos-fechados então por definição X é zero-dimensional. ∎

Lema 12 *Todo subespaço Y de um espaço topológico zero-dimensional X é zero-dimensional.*

Prova Seja $(O_i)_{i \in I}$ uma base para os subconjuntos abertos de X formada por conjuntos abertos-fechados. A família $(O_i \cap Y)_{i \in I}$ é uma base para os subconjuntos de Y. Mas estes conjuntos abertos também são subconjuntos fechados de Y, já que eles são formados por interseções com Y de subconjuntos fechados de X. Logo, Y é zero-dimensional. ∎

Definição 17 *Um espaço topológico zero-dimensional compacto é chamado **espaço Booleano**.*

Seja $(X_i)_{i \in I}$ uma família de espaços topológicos. No produto $\prod_{i \in I} X_i$ desta família, podemos definir uma topologia tomando como base conjuntos abertos com todos os subconjuntos da forma $(O_i)_{i \in I}$ onde, para cada índice $i \in I$, O_i é uma subconjunto aberto de X_i, mas para um número finito de índices i, temos $O_i \neq X_i$. É fácil verificar que a coleção formada pela união de conjuntos deste tipo é fechado sob as interseções e uniões arbitrárias. Esta é a coleção de conjuntos que tomamos como a família de abertos para a topologia $(X_i)_{i \in I}$. A topologia definida desta maneira é chamada de **topologia produto**.

Apresentaremos a seguir, sem sua demonstração, um importante resultado, conhecido como teorema de Tychonoff.

Teorema 13 ***(Tychonoff)*** *O produto de espaços topológicos compactos é um espaço topológico compacto.*

Examinemos agora o caso em que cada X_i na família de espaços $(X_i)_{i\in I}$ é o conjunto $\{\mathbf{0{,}1}\}$ com a topologia **discreta** (aquela em que todos os subconjuntos são abertos).

Neste caso, o produto $\prod_{i\in I} X_i$ é o conjunto $\{\mathbf{0{,}1}\}^I$ de aplicações de I sobre $\{\mathbf{0{,}1}\}$.

Para produzir um conjunto aberto básico Ω na topologia produto, devemos tomar um número finito de índices, $i_1, i_2, ..., i_k$ em I e conjuntos abertos $O_{i_1}, O_{i_2}, ..., O_{i_k}$ de $\{\mathbf{0{,}1}\}$, no qual, neste caso, são subconjuntos arbitrários de $\{\mathbf{0{,}1}\}$, que definem

$$\Omega = \{\mathbf{0{,}1}\}^{I-\{i_1,i_2,...,i_k\}} \times O_{i_1} \times O_{i_2} \times ... \times O_{i_k},$$

ou alternativamente

$$\Omega = \{f \in \{\mathbf{0{,}1}\}^I : f(i_1) \in O_{i_1}\,,\ f(i_2) \in O_{i_2}\,,\ ... \text{ e } f(i_k) \in O_{i_k}\}.$$

É natural supor que estamos interessados apenas nos índices i_j que correspondem a conjuntos abertos diferentes do conjunto $\{\mathbf{0{,}1}\}$ propriamente. É inútil considerar o caso em que um dos O_{i_j} seja vazio, pois assim teríamos $\Omega = \emptyset$. Restando portanto, somente duas possibilidades para O_{i_j}: $O_{i_j} = \{\mathbf{0}\}$ ou $O_{i_j} = \{\mathbf{1}\}$.

Assim vemos que para produzir uma conjunto aberto básico Ω na topologia produto em $\{\mathbf{0{,}1}\}$, devemos tomar um número finito de índices $i_1, i_2, ..., i_k$ em I e o mesmo número de elementos $\epsilon_1, \epsilon_2, ..., \epsilon_k$ em $\{\mathbf{0{,}1}\}$ e definir

$$\Omega = \{f \in \{\mathbf{0{,}1}\}^I : f(i_1) = \epsilon_1 \text{ e } f(i_2) = \epsilon_2 \text{ e ... e } f(i_k) = \epsilon_k\}.$$

Um conjunto aberto básico, portanto, é o conjunto de todas as aplicações de I sobre $\{\mathbf{0{,}1}\}$ que assume valores dados em um número finito de pontos.

Note que o complemento em $\{\mathbf{0{,}1}\}^I$ do conjunto Ω pode ser considerado como o seguinte conjunto:

$$\bigcup_{1\leq j\leq k}\{f \in \{\mathbf{0{,}1}\}^I : f(i_j) = 1 - \epsilon_j\}.$$

Como esta união de k conjuntos abertos básicos, é claramente um conjunto aberto. Podemos concluir que Ω é um conjunto fechado.

Os conjuntos abertos na topologia $\{\quad\}$ são portanto conjuntos abertos-fechados. Consequentemente, provamos que:

Lema 14 *O espaço topológico $\{\boldsymbol{0{,}1}\}^I$ é zero-dimensional.*

Como o espaço discreto $\{\mathbf{0{,}1}\}$ é claramente compacto, podemos concluir, usando o teorema de Tychonoff, que:

Lema 15 *O espaço $\{\boldsymbol{0{,}1}\}^I$ é um espaço topológico Booleano.*

3.4.2 Compacidade do cálculo proposicional

O teorema que apresentaremos a seguir denota uma importante propriedade para a lógica de predicados, pois garante que toda e qualquer fórmula é derivável (ou logicamente implicada, no caso semântico) a partir de um conjunto finito de premissas.

O teorema de Tychonoff nos permite dar uma rápida prova do teorema de compacidade do cálculo proposicional. Que se segue:

Teorema 16 ***(Compacidade do cálculo proposicional)*** *Para qualquer conjunto $\mathcal{P}$ de fórmulas do cálculo proposicional, $\mathcal{P}$ é contraditório se e somente se pelo menos um subconjunto finito de $\mathcal{P}$ é contraditório.*

Prova Seja P um conjunto de variáveis proposicionais e denotemos por $\mathcal{P}$ o conjunto de fórmulas. Para cada $p \in \mathcal{P}$, denotemos por $\Delta(p)$ o conjunto de valorações que o satisfaz:

$$\Delta(p) = \{\delta \in \{\mathbf{0{,}1}\}^P : \bar{\bar{\delta}}(p) = 1\}.$$

Se $A_1, A_2, ..., A_n$ são variáveis que ocorrem na fórmula p, vemos que $\Delta(p)$ é a união dos conjuntos da forma

$$\left\{\delta \in \{\mathbf{0{,}1}\}^I : \delta(A_1) = \epsilon_1 \text{ e } \delta(A_2) = \epsilon_2 \text{ e ... e } \delta(A_k) = \epsilon_k\right\}$$

onde os ϵ_i são elementos de $\{\mathbf{0{,}1}\}$.

Na verdade, a consistência da fórmula p pela valoração δ não depende do valor que δ assume fora do conjunto $\{A_1, A_2, ..., A_n\}$.

Portanto, o conjunto $\Delta(p)$ é a união de conjuntos abertos básicos no espaço topológico $\{\mathbf{0{,}1}\}^P$. Esta é uma união finita: que envolve no máximo 2^n conjuntos. Logo, podemos concluir que $\Delta(p)$ é um conjunto aberto-fechado.

Agora considere o conjunto de fórmulas $T \subseteq \mathcal{P}$ que não é consistente. Isto signinifica precisamente, que a interseção, $\bigcap_{p \in T} \Delta(p)$, é um conjunto vazio. Assim a família $(\Delta(p))_{p \in T}$ é, no espaço compacto $\{\mathbf{0{,}1}\}^P$, uma família de conjuntos fechados cuja interseção é vazia. Logo, é possível extrair uma subfamília finita cuja interseção seja vazia; então existe um subconjunto finito $T_0 \subseteq T$ tal que $\bigcap_{p \in T_0} \Delta(p) = \emptyset$.

Isto significa que existem subconjuntos finitos de T que não são consistentes, provando portanto, o teorema de compacidade do cálculo proposicional.
∎

3.4.3 Álgebra de Boole como anel

Definiremos neste texto a álgebra de Boole como anel e conheceremos alguns resultados interessantes sobre esta álgebra. Seguindo a definição encontraremos uma construção da lógica clássica como uma álgebra Booleana.

Definição 18 *Uma* ***álgebra de Boole*** *(também chamado de* ***anel booleano****) é um anel $\langle A, +, \times, \mathbf{0}, \mathbf{1} \rangle$ no qual cada elemento é idempotente para a multiplicação (ou seja, é igual ao seu quadrado).*

Considerando o conjunto P de variáveis proposicionais e o conjunto associado de fórmulas $\mathcal{P}$. O conjunto quociente $\mathcal{P}/\sim$, ou seja, o conjunto de classes de fórmulas logicamente equivalentes (as classes de equivalência de $\mathcal{P}$ serão representadas por $cl(\mathcal{P})$) com as operações $\not\Leftrightarrow$ e $\wedge$, tem a estrutura de uma álgebra de Boole (estas operações podem ser definidas neste conjunto porque a relação $\sim$ é compatível com os conectivos proposicionais). A classe $\mathbf{0}$ de **antitautologias** e a classe $\mathbf{1}$ de **tautologias** são respectivamente, o elemento identidade para as operações $\not\Leftrightarrow$ e $\wedge$.

Lema 17
1. *Em qualquer álgebra de Boole, todo elemento é seu próprio inverso aditivo.*
2. *Toda álgebra de Boole é comutativa.*

Prova Seja $\langle A, +, \times, \mathbf{0}, \mathbf{1} \rangle$ uma álgebra de Boole e seja x e y elementos de A. Por definição, temos que $x^2 = x$ e $y^2 = y$ e $(x+y)^2 = (x+y)$, enquanto, como um anel qualquer, temos

$$
\begin{aligned}
(x+y)^2 &= x^2 + xy + yx + y^2 \\
x + y &= x + xy + yx + y \\
xy + yx &= \mathbf{0}
\end{aligned}
$$

Tomando $y = \mathbf{1}$, obtemos um resultado particular que é $x + x = 0$ ou $x = -x$ o que prova o primeiro item.

Para x e y arbitrários, já sabemos que xy é o inverso aditivo de xy. Mas como $xy + yx = 0$, temos que yx também é um inverso de xy. Assim podemos concluir que $xy = yx$ e portanto, a álgebra é comutativa. ∎

Seja $\langle A, +, \times, \mathbf{0}, \mathbf{1} \rangle$ uma álgebra Booleana. Defina uma relação binária $\leq$ em A como se segue: para todos os elementos x e y de A, $x \leq y$ se e somente se $xy = x$. Verificaremos que isto na verdade é uma relação de ordem. Para todos os elementos x, y e z de A, temos

- $x \leq x$, já que $x^2 = x$ por definição;

- se $x \leq y$ e $y \leq z$, então $xy = x$ e $yz = y$; logo, $xz = (xy)z = x(yz) = xy = x$, então $x \leq z$;
- se $x \leq y$ e $y \leq x$, então $xy = x$ e $yx = y$, portanto $x = y$ por comutatividade.

Logo a relação $\leq$ é reflexiva, transitiva, e antissimétrica.

Os seguintes teoremas listam algumas das principais propriedades desta relação de ordem.

Teorema 18 *0 é o **menor elemento** e 1 é o **maior elemento** da relação $\leq$.*

Prova
Na verdade, para todo x, $0 \times x = 0$ e $1 \times x = x$, portanto $0 \leq x$ e $x \leq 1$. ▮

Teorema 19 *Quaisquer dois elementos x e y de A tem um **maior limite inferior** (ou seja, um limite inferior comum que é maior que qualquer outro limite inferior comum, também chamado de **ínfimo**), denotado por $x \frown y$: especificamente, o produto xy.*

Prova Temos que $(xy)x = x^2y = xy$ e $(xy)y = xy^2 = xy$, assim xy é um limite inferior de x e de y. Se z é um limite inferior comum de x e y, temos $zx = z$ e $zy = z$, assim $z(xy) = (zx)y = zy = z$, o que significa que $z \leq xy$; assim concluimos que xy é o maior limite inferior de x e y. ▮

Teorema 20 *Quaisquer dois elementos x e y de A tem um **menor limite superior** (ou seja, um limite superior comum que é menor que qualquer outro limite superior comum, também chamado de **supremo**), denotado por $x \smile y$: especificamente, o elemento $x + y + xy$.*

Prova Na verdade,

$$x(x + y + xy) = x^2 + xy + x^2y = x + xy + xy = x + 0 = x,$$
$$y(x + y + xy) = yx + y^2 + yxy = yx + y + xy = y + 0 = y.$$

Portanto, temos $x \leq x + y + xy$ e $y \leq x + y + xy$. Agora, se z é um elemento de A tal que $x \leq z$ e $y \leq z$, temos que, $xz = x$ e $yz = y$, então

$$(x + y + xy)z = xz + yz + xyz = x + y + xy,$$

logo, $x + y + xy \leq z$; assim $x + y + xy$ é o menor limite superior comum a x e y. ▮

Teorema 21 *Cada uma das operações* $\frown$ *e* $\smile$ *é distributiva sobre a outra.*
Prova Dados x, y e z de A. Temos,

$$\begin{aligned} x \frown (y \smile z) &= x(y+z+yz) \\ &= xy+xz+xyz \\ &= xy+xz+xy\cdot xz \\ &= (x\frown y)\smile(x\frown z) \end{aligned}$$

Por outro lado, também temos

$$\begin{aligned} (x\smile y)\frown(x\smile z) &= (x+y+xy)(x+z+xz) \\ &= x^2+xz+x^2z+yx+yz+yxz+x^2y+xyz+x^2yz \\ &= x+yz+xyz \\ &= x\smile(yz) \\ &= x\smile(y\frown z) \end{aligned}$$

Provando portanto, a distributividade das duas operações. ∎

Teorema 22 *Para todo elemento* $x \in A$*, há uma elemento* $x' \in A$ *chamado o* ***complemento*** *de* x*, tal que* $x \smile x' = 1$*, e* $x \frown x' = 0$*.*

Prova Se tal elemento x' existe, ele satisfaz $xx' = 0$ e $x + x' + xx' = 1$, portanto $x + x' = 1$, ou também $x' = 1 + x$. Portanto,

$$x \smile (1+x) = x + (1+x) + x(1+x) = x+1+x+x+x^2 = 1$$
$$x \frown (1+x) = x(1+x) = x + x^2 = 0$$

Assim estabelecemos não somente a existência mas também a unicidade do complemento de x: que é $1 + x$. ∎

3.4.4 Álgebra de Boole como conjunto ordenado

As propriedades demonstradas nos teoremas da seção anterior caracterizam a álgebra de Boole. Iremos agora, apresentar um segundo método para definir a álgebra de Boole.

Propriedade 1 *Seja* $\langle A, \leq\rangle$ *um conjunto ordenado com as seguintes propriedades:*

1. *existe um menor elemento (denotado por 0) e um maior elemento (denotado por 1);*
2. *quaisquer dois elementos* x *e* y *tem um menor limite superior (denotado por* $x \smile y$*) e um maior limite inferior (denotado* $x \frown y$*);*

3. *cada operação $\smile$ e $\frown$ é distributiva uma sobre a outra;*
4. *para todo elemento x em A, há pelo menos um elemento x' em A tal que $x \smile x' = 1$ e $x \frown x' = 0$.*

O conjunto ordenado que tem as propriedades (1) e (2) é chamado de **reticulado**. Se também tem-se a propriedade (3), o conjunto e chamado de **reticulado distributivo**. Se as propriedades (1), (2) e (4) são satisfeitas, dizemos que é uma **reticulado complementado**, onde o **complemento** de um elemento x é o único elemento x' no qual $x \smile x' = 1$ e $x \frown x' = 0$.

O complemento do elemento x será denotado por x^C. Claramente temos que $1^C = 0$ e $0^C = 1$. Observe que como uma das consequências da unicidade do complemento, a aplicação $x \mapsto x^C$ de A sobre A é uma bijeção que é igual ao seu próprio inverso (para todo x, $(x^C)^C = x$).

Agora estabeleceremos o que é normalmente conhecido como a **Lei de De Morgan**:

Lema 23 *Para qualquer elemento x e y de A.*

$$\begin{array}{c} (x \frown y)^C = x^C \smile y^C \text{ e} \\ (x \smile y)^C = x^C \frown y^C. \end{array}$$

Prova Note que, para mostrar $x^C \smile y^C$ é uma complemento de $x \frown y$, basta provar que $(x^C \smile y^C) \smile (x \frown y) = 1$ e $(x^C \smile y^C) \frown (x \frown y) = 0$. De fato, pois

$$\begin{array}{rcl} (x^C \smile y^C) \smile (x \frown y) & = & (x^C \smile y^C \smile x) \frown (x^C \smile y^C \smile y) \\ & = & (1 \smile y^C) \frown (x^C \smile 1) = 1 \frown 1 = 1; \\ (x^C \smile y^C) \frown (x \frown y) & = & (x^C \frown y \frown x) \smile (y^C \frown x \frown y) \\ & = & (0 \frown y) \smile (0 \frown x) = 0 \smile 0 = 0. \end{array}$$

De maneira análoga demonstramos a segunda lei, já que

$$\begin{array}{rcl} (x^C \frown y^C) \smile (x \smile y) & = & (x^C \smile x \smile y) \frown (y^C \smile x \smile y) \\ & = & (1 \smile y) \frown (x \smile 1) = 1 \frown 1 = 1; \\ (x^C \frown y^C) \frown (x \smile y) & = & (x^C \frown y^C \frown x) \smile (x^C \frown y^C \frown y) \\ & = & (y^C \frown 0) \smile (x^C \frown 0) = 0 \smile 0 = 0. \end{array}$$

∎

A lei de De Morgan pode ser imediatamente generalizada (por indução) como se segue:

Lema 24 *Para qualquer inteiro $K \geq 1$ e elementos $x_1, x_2, ..., x_k$ de A,*

$$(x_1 \frown x_2 \frown ... \frown x_k)^C = x_1^C \smile x_2^C \smile ... \smile x_k^C \text{ e}$$
$$(x_1 \smile x_2 \smile ... \smile x_k)^C = x_1^C \frown x_2^C \frown ... \frown x_k^C.$$

Definição 19 *Um elemento A em uma álgebra de Boole $\langle A, \smile, \frown, 0, 1\rangle$ é chamado* ***átomo*** *se e somente se é não nulo e não tem um limite inferior estrito não nulo.*

Em outras palavras, a é um átomo se e somente se $a \neq 0$ e, para todo elemento b em A, se $b \leq a$, então ou $b = a$ ou $b = 0$.

A relação de ordem nesta álgebra de Boole é a seguinte:
Se G e H são fórmulas, então $cl(G) \leq cl(H)$ se e somente se a fórmula $(G \Rightarrow H)$ é uma tautologia.

Lema 25 *Existe uma álbegra Booleana sem átomos: Esta situação ocorre com a álgebra de Boole $\mathcal{P}/\sim$ de classe de equivalência das fórmulas do cálculo proposicional onde o conjunto P de variáveis proposicionais é infinito.*

Prova Para provar que não há átomos em $\mathcal{P}/\sim$, mostraremos que todo elemento não nulo tem um limite inferior estrito diferente de 0. Considere uma fórmula G tal que $cl(G) \neq 0$, tal que $\neg G$ não é uma tautologia, ou equivalentemente, que existe pelo menos uma valoração para P que satisfaz G. Escolha tal atribuição e denote-a por δ. Também escolha uma variável proposicional X que não ocorre na fórmula G. Isto é possível porque P é infinito.

Denotemos por H a fórmula $(G \wedge X)$. Obviamente temos $\vdash^* ((G \wedge X) \Rightarrow G)$, portanto $cl(H) \leq cl(G)$. A atribuição de valores de verdade λ que é definida por:

Para todo $Y \in P$,

$$\lambda(Y) = \begin{cases} \delta(Y) & \text{se } Y \neq X \\ \mathbf{1} & \text{se } Y = X \end{cases}$$

satisfaz G (desde que X não ocorra em G) e satisfaz X, então satifaz H. Portanto $cl(H) \neq 0$. Por outro lado, a valoração μ definida por:

Para todo $Y \in P$,

$$\mu(Y) = \begin{cases} \delta(Y) & \text{se } Y \neq X \\ \mathbf{0} & \text{se } Y = X \end{cases}$$

satisfaz G (pela mesma razão que λ o faz) mas não satisfaz H, portanto não satisfaz a fórmula $(G \Rightarrow H)$. Então não temos $cl(G) \leq cl(H)$, o que mostra que $cl(H)$ é um limite inferior estrito para $cl(G)$, portanto ele é um estrito, limite inferior não nulo. ∎

Definição 20 *Uma álgebra Boolena é* ***atômica*** *se e somente se todo elemento não nulo tem pelo menos um átomo menor que ele.*

Teorema 26 *Toda álgebra de Boole finita é atômica.*

Prova Seja $\langle A, \smile, \frown, 0, 1\rangle$ uma álgebra de Boole finita e seja x um elemento não nulo de A. Denote por $m(x)$ o conjunto de limites inferiores estritos não nulos de x em A. Se $m(x)$ é vazio, então x é um átomo. Se $m(x)$ não é vazio, então por ser finito, pelo menos um dos elementos é minimal na ordem $\leq$, ou seja, nenhum elemento de $m(x)$ é estritamente menor que ele. E fácil ver que este tal elemento minimal é um átomo de A que é menor que x. ∎

3.4.5 Filtros e ultrafiltros

Os temas abordados aqui serviram como base para a construção do importante teorema de Stone que será apresentado na próxima seção. Começaremos pela definição de filtro e posteriormente, ultrafiltro.

Definição 21 *Um* ***filtro*** *em uma álgebra de Boole* $\mathcal{A} = \langle A, +, \times, 0, 1\rangle$ *é um subconjunto* F *de* A *tal que o conjunto*

$$\left\{x \in A : x^C \in F\right\}$$

é uma ideal em $\mathcal{A}$.

Seja F um filtro em uma álgebra de Boole $\mathcal{A} = \langle A, +, \times, 0, 1\rangle$. Seja I o ideal $\left\{x \in A : x^C \in F\right\}$. I é formado pela imagem inversa de F sobre a operação de complementação: $x \mapsto x^C$. Porém, como esta operação é uma involução (uma bijeção cujo inverso é ele mesmo), temos que I é o conjunto de complementos de F e F o conjunto de complementos de I. O ideal I é chamado de **ideal dual** do filtro F.

Teorema 27 *Seja* $\mathcal{A} = \langle A, \leq, 0, 1\rangle$ *uma álgebra de Boole e* F *um subconjunto de* A*. Para* F *ser um filtro, é necessário e suficiente que as seguintes condições sejam satisfeitas:*

1. $0 \notin F$ *e* $1 \in F$*;*
2. *para todos os elementos* x *e* y *de* F*,* $x \frown y \in F$*;*
3. *para todo* $x \in F$ *e para todo* $y \in A$*, se* $y \geq x$*, então* $y \in F$*.*

Prova Seja $I = \{x \in A : x^C \in F\}$. Se F é um filtro, então temos que I é um ideal dual. Assim, como um ideal temos que: $0 \in I$, portanto $1 = 0^C \in F$. E $1 \notin I$, logo $0 = 1^C \notin F$. O que prova (1).

Se x e $y \in F$, então x^C e $y^C \in I$. Portanto, $x^C y^C \in I$ e
$x^C \smile y^C = x^C + y^C + x^C y^C \in I$.
Como $x^C \smile y^C = (x \frown y)^C$, podemos concluir que $x \frown y \in F$. O que satisfaz (2).

Agora se $x \in F$, $y \in A$ e $y \geq x$, temos que:

$$\begin{aligned} xy &= x \\ (x \frown y) &= x \\ \\ (x \frown y)^C &= x^C \\ x^C \smile y^C &= x^C \\ x^C + y^C + x^C y^C &= x^C \\ y^C + x^C y^C &= 0 \\ x^C y^C &= -y^C = y^C \end{aligned} \tag{2}$$

portanto, concluimos que $y^C \leq x^C$ e $y^C \in I$ logo $y \in F$. O que prova (3). ∎

Definição 22 *Em uma álgebra de Boole, um* ***ultrafiltro*** *é um filtro* ***maximal****, ou seja, um filtro que não está estritamente contido em outro filtro qualquer.*

Está claro que, do ponto de vista da dualidade, ultrafiltros correspondem a ideais maximais.

Teorema 28 *Para todo anel Booleano $\mathcal{A} = \langle A, +, \times, 0, 1\rangle$, para todo ideal $F \in \mathcal{A}$, e para todo inteiro $k \geq 2$, as propriedades seguintes são equivalentes:*

1. *F é um ultrafiltro;*
2. *existe um homomorfismo h de $\mathcal{A}$ sobre $\{0, 1\}$ tal que*
$$F = \{x \in A : h(x) = 1\};$$
3. *para todo elemento x em A, $x \in F$ ou $1 + x \in F$;*
4. *para todos os elementos x e y de A, se $x \smile y \in F$, então $x \in F$ ou $y \in F$;*

5. *para todos os elementos* $x_1, x_2, ..., x_k$ *em* A, *se* $x_1 \smile x_2 \smile ... \smile x_k \in F$, *então* $x_1 \in F$ *ou* $x_2 \in F$ *ou ... ou* $x_k \in F$.

Definição 23 *Em uma álgebra de Boole* $\langle A, \leq, 0, 1\rangle$ *uma* ***base para o filtro (filtro-base)*** *é um subconjunto de* A *que tem as seguintes propriedades, conhecidas como a* ***propriedade da interseção finita****: todo subconjunto finito não vazio de* B *tem um maior limite inferior não vazio.*

Em outras palavras, $B \subseteq A$ é uma filtro-base se e somente se: para qualquer inteiro $k \geq 1$ e quaisquer elementos $x_1, x_2, ..., x_k$ de B, $x_1 \frown x_2 \frown ... \frown x_k \neq 0$.

Lema 29 *Seja* $\langle A, \leq, 0, 1\rangle$ *uma álgebra de Boole e seja* X *um subconjunto de* A. *Para a existência de um filtro em* $\mathcal{A}$ *que inclui* X, *é necessário e sufuciente que* X *seja um filtro-base.*

Prova Se X está em um filtro F, e se $x_1, x_2, ..., x_k$ são elementos de X, então o ínfimo $x_1 \frown x_2 \frown ... \frown x_k$ pertence a F, e como $0 \notin F$, este ínfimo é não-nulo, assim X é um filtro-base. Agora suponha que X é um filtro-base.

- Se $X = \emptyset$, $\{1\}$ é um filtro em $\mathcal{A}$ que inclui X.
- Se X não é vazio, defina

$$F_X = \{x \in A : (\exists k \in N^*) \, (\exists x_1 \in X) \, (\exists x_2 \in X) \\ ... \, (\exists x_k \in X) \, (x \geq x_1 \frown x_2 \frown ... \frown x_k) \; \}.$$

Então F_X é formado pelos ínfimos dos subconjuntos finitos não vazios de X junto com todos os elementos maiores ou iguais a um destes ínfimos. Em particular, cada elemento de X pertence a F_X, portanto F_X inclui X. É fácil ver que F_X é um filtro. De fato,

1. $0 \notin F_X$, pois do contrário a propriedade de interseção finita não é verdade para X. E $1 \in F_X$, já que X é não vazio e pelo menos um elemento de X é menor ou igual a 1.
2. Se $x \geq x_1 \frown x_2 \frown ... \frown x_k$ e $y \geq y_1 \frown y_2 \frown ... \frown y_k$, então temos

$$x \frown y \geq x_1 \frown x_2 \frown ... \frown x_k \frown y_1 \frown y_2 \frown ... \frown y_k,$$

   portanto, $x \frown y \in F_X$.
3. Se $x \geq x_1 \frown x_2 \frown ... \frown x_k$ e $y \geq x$, então $y \geq x_1 \frown x_2 \frown ... \frown x_k$ consequentemente $y \in F_X$.

Assim, temos que F_X é um filtro que contém X. ∎

3.4.6 Teorema de Stone

Dada uma álgebra de Boole $\mathcal{A} = \langle A, +, -, 0, 1\rangle$, seja $\mathcal{F}(\mathcal{A})$ a classe de todos os filtros primos de $\mathcal{A}$. Para cada $a \in \mathcal{A}$, seja $h(a)$ o conjunto de todos os filtros F de $\mathcal{F}(\mathcal{A})$ para os quais $a \in F$ e, finalmente, seja $\mathrm{P}(\mathcal{A})$ a classe de todos os conjuntos $h(a)$ tais que $a \in \mathcal{A}$.

O Teorema do Isomorfismo de Stone nos garante que h é um isomorfismo Booleano de $\mathcal{A}$ sobre $\mathrm{P}(\mathcal{A})$, ou seja, toda álgebra Booleana é isomorfa a um corpo de conjuntos, isto é, a uma coleção não vazia de subconjuntos de um conjunto X, fechada em relação às operações de união, interseção e complemento.

Definição 24 *O conjunto de homomorfismos de uma álgebra de Boole $\mathcal{A}$ sobre $\{0, 1\}$ é denotado por $S(\mathcal{A})$ e é chamada de **espaço Stone de** $\mathcal{A}$.*

O conjunto $S(\mathcal{A})$ é um subconjunto de $\{0, 1\}^A$, o conjunto de aplicações de A sobre $\{0, 1\}$. É um espaço topológico ao pegarmos a topologia discreta em $\{0, 1\}$ e darmos a ela a topologia produto. Então podemos ter $S(\mathcal{A})$ como uma topologia induzida por $\{0, 1\}^A$. Os subconjuntos abertos de $S(\mathcal{A})$ são interseções com $S(\mathcal{A})$ de subconjuntos abertos de $\{0, 1\}^A$.

Lema 30 *O espaço topológico $S(\mathcal{A})$ é zero-dimensional.*

Prova Pelo lema (14) sabemos que $\{0, 1\}^A$ é zero-dimensional. Portanto, considere uma base $(\Omega_i)_{i \in I}$ para o espaço $\{0, 1\}^A$ formada por conjuntos Cada Ω_i é o conjunto de todas as aplicações de A sobre $\{0, 1\}$ que assumem um valor específico em um certo número finito de pontos.

Para cada i, defina $\Gamma_i = \Omega_i \cap S(\mathcal{A})$, como na demonstração lema (12), a família $(\Gamma_i)_{i \in I}$ é uma base para o conjunto de abertos de $S(\mathcal{A})$ formada por conjuntos abertos-fechados. Cada Γ_i é um conjunto de homomorfismos de álgebras de Boole de $\mathcal{A}$ sobre $\{0, 1\}$ que assumem certos valores em um número finito de ponto dados. Onde concluimos que $S(\mathcal{A})$ é zero-dimensional.

∎

Lema 31 *Para que um subconjunto Δ de $S(\mathcal{A})$ seja uma base de um conjunto de abertos, é necessário e suficiente que exista um elemento **a** em A tal que*

$$\Delta = \{h \in S(\mathcal{A}) : h(a) = 1\}$$

Mais, quando esta condição é satisfeita, tal elemento é único.

Prova

- *Suficiente*: Suponha que $\Delta = \{h \in S(\mathcal{A}) : h(a) = 1\}$; Δ é o conjunto de homomorfismos de A sobre $\{0,1\}$ que assumem o valor 1 no ponto a: então esta é um dos conjuntos abertos básicos em $S(\mathcal{A})$.
- *Necessário*: Suponha que Δ é um subconjunto aberto básico de $S(\mathcal{A})$.
  - Se $\Delta = \emptyset$, então $\Delta = \{h \in S(\mathcal{A}) : h(0) = 1\}$.
  - Se $\Delta \neq \emptyset$, então há um inteiro $n \geq 1$, elementos $a_1, a_2, ..., a_n$ em A e elementos $\epsilon_1, \epsilon_2, ..., \epsilon_n$ em $\{0,1\}$ tal que
    $$\Delta = \{h \in S(\mathcal{A}) : h(a_1) = \epsilon_1 \quad e \quad h(a_2) = \epsilon_2 \quad e \ldots e \quad h(a_n) = \epsilon_n\}$$
    Para todo $k \in \{1, 2, ..., n\}$, defina
    $$b_k = \begin{cases} a_k & \text{se} \quad \epsilon_k = 1 \\ 1 + a_k & \text{se} \quad \epsilon_k = 0 \end{cases}$$
    Para todo homomorfismo $h \in S(\mathcal{A})$ e para todo $K \in \{1, 2, ..., n\}$, temos
    $$h(b_k) = \begin{cases} h(a_k) & \text{se} \quad \epsilon_k = 1 \\ 1 + h(a_k) & \text{se} \quad \epsilon_k = 0 \end{cases}$$
    Com isto temos que para $h \in S(\mathcal{A})$, $h \in \Delta$ se e somente se $h(b_k) = 1$ para todo $k \in \{1, 2, ..., n\}$. O que significa que
    $$h(b_1) \frown h(b_2) \frown ... \frown h(b_n) = 1;$$
    $$h(b_1 \frown b_2 \frown ... \frown b_n) = 1$$
    já que h é um homomorfismo. Assim, vemos que, definindo $a = b_1 \frown b_2 \frown ... \frown b_n$, temos
    $$\Delta = \{h \in S(\mathcal{A}) : h(a) = 1\}.$$
- *Unicidade*: Se a e b são elementos distintos de A, então $a + b \neq 0$; então podemos considerar o filtro principal gerado por $a + b$ e um ultrafiltro que inclui este filtro. Para tal ultrafiltro, existe uma homomorfismo associado ϕ de $\mathcal{A}$ sobre $\{0,1\}$ que satisfaz $\phi(a + b) = 1$, ou seja, $\phi(a) + \phi(b) = 1$. O que significa que um dos dois elementos $\phi(a)$ ou $\phi(b)$ é igual a 1. Provando que
  $$\{h \in S(\mathcal{A}) : h(a) = 1\} \neq \{h \in S(\mathcal{A} : h(b) = 1)\}$$
  já que ϕ pertence a apenas um destes conjuntos.

∎

Lema 32 *O conjunto de subconjuntos abertos-fechados de $S(\mathcal{A})$ coincide com o conjunto de conjuntos abertos básico.*

Prova Nós sabemos pelo lema (30) que todos os conjuntos abertos básicos são abertos-fechados. Reciprocamente, seja Γ um subconjunto aberto-fechado arbitrário de $S(\mathcal{A})$. Como Γ é aberto, ele é uma união de conjuntos de abertos básicos: por exemplo, $\Gamma = \bigcup_{i \in J} \Gamma_i$ para algum subconjunto $J \subseteq I$. Mas desde que Γ é um subconjunto fechado de uma espaço compacto $S(\mathcal{A})$, é também compacto. Então da cobertura aberta $(\Gamma_i)_{i \in J}$ de Γ, podemos extrair uma subcobertura finita, por exemplo: $\Gamma = \Gamma_{j_1} \cup \Gamma_{j_2} \cup ... \cup \Gamma_{j_m}$. Sabemos (pelo lema 31) que podemos encontrar elementos $x_1, x_2, ..., x_m$ em A tal que

$$\text{para todo } k \in \{1, 2, ..., m\},\ \Gamma_{j_k} = \{h \in S(\mathcal{A}) : h(x_k) = 1\}.$$

Sejam $x = x_1 \smile x_2 \smile ... \smile x_k$ e $\Delta = \{h \in S(\mathcal{A}) : h(x) = 1\}$. Mostraremos que $\Gamma = \Delta$. Todo elemento de Γ é um homomorfismo que assume o valor 1 em pelo menos um dos pontos $x_1, x_2, ..., x_m$; portanto também assume valor 1 em x que o supremo deles, assim $\Gamma \subseteq \Delta$.

Por outro lado, qualquer homomorfismo que não está em Γ, e então não assume valor 1 em nenhum dos pontos $x_1, x_2, ..., x_m$, deve assumir o valor 0 em cada um dos pontos, e também no ponto x que o supremo, logo não pertence a Δ. Isto prova que $\Delta \subseteq \Gamma$. Então, $\Gamma = \Delta$ e como Δ é um conjunto aberto básico, Γ é único. ∎

Teorema 33 ***(Teorema de Stone)***
Toda álgebra de Boole é isomorfa à álgebra de Boole do subconjunto de abertos-fechados do espaço de Stone.

Prova
A álgebra de Boole dos subconjuntos abertos-fechados de $S(\mathcal{A})$ é denotada por $\mathcal{B}(S(\mathcal{A}))$. Seja H a aplicação de A sobre $\wp(S(\mathcal{A}))$ que, para cada elemento a em A, associa

$$H(a) = \{h \in S(\mathcal{A}) : h(a) = 1\}.$$

Vamos mostrar que H é um isomorfismo de álgebra de Boole de A sobre $\mathcal{B}(S(\mathcal{A}))$. Pelos lemas (31) e (32), a aplicação H assume seus valores em $\mathcal{B}(S(\mathcal{A}))$ e sua imagem é todo o $\mathcal{B}(S(\mathcal{A}))$.
Então H é uma sobrejeção de A sobre $\mathcal{B}(S(\mathcal{A}))$. Para mostrar que H é um isomorfismo de álgebras de Boole, basta ver que para todos os elementos x e y em A, $x \leq y$ se e somente se $H(x) \subseteq H(y)$. Então seja x e y dois elementos de A. Se $x \leq y$, então para qualquer homomorfismo h que satisfaz $h(x) = 1$, temos

$$\begin{aligned} xy &= x \\ h(xy) &= h(x) \\ h(x)h(y) &= h(x) \\ 1 \cdot h(y) &= 1 \\ h(y) &= 1 \end{aligned}$$

o que significa que $H(x)$ é um subconjunto de $H(y)$.

Se x não é menor ou igual a y, então $x \geq y$ e por definição $xy = y$ e portanto $y(1+x) = 0$, logo seu complementar $(1+y)x \neq 0$. Assim, podemos considerar o filtro principal gerado por $x(1+y)$, um ultrafiltro que o inclui e o homomorfismo $h \in S(\mathcal{A})$ associado a este ultrafiltro. Temos $h(x(1+y)) = 1$, portanto $h(x) = 1$ e $h(1+y) = 1$, logo $h(y) = 0$. Concluimos que $h \in H(x)$ e $h \notin H(y)$, e então $H(x)$ não está contido em $H(y)$.

∎

Teorema 34 *Todo Espaço topológico Booleano X é homeomorfo a um espaço de Stone $\mathcal{S}(\mathcal{B}(X))$ de uma álgebra de Boole de subconjuntos abertos-fechados de X.*

Prova Seja X um espaço Booleano. Tomemos a álgebra de Boole $\mathcal{B}(X)$ de subconjuntos abertos-fechados de X como uma base para os conjuntos abertos na topologia em X.
Para cada $x \in X$, denotemos f_x como a aplicação de $\mathcal{B}(X)$ sobre $\{0,1\}$ definida por

$$f_x(\Omega) = \begin{cases} 1 & \text{se} \quad x \in \Omega; \\ 0 & \text{se} \quad x \notin \Omega. \end{cases}$$

Agora basta mostrar que a aplicação f que, para cada $x \in X$, associa f_x é uma homeomorfismo do espaço topológico X sobre o espaço topológico $\mathcal{S}(\mathcal{B}(X))$.

- *Para cada $x \in X$, f_x é um homomorfismo de álgebras de Boole;*
  De fato, para quaisquer subconjuntos aberto-fechado Ω e Δ de X, temos que $f_x(\Omega \cap \Delta) = 1$, se e somente se, $x \in \Omega \cap \Delta$, ou seja, $x \in \Omega$ e $x \in \Delta$. Que é equivalente a dizer que: $f_x(\Omega) = 1$ e $f_x(\Delta) = 1$ logo,

  $$f_x(\Omega) f_x(\Delta) = 1.$$

  Consequentemente,

  $$f_x(\Omega \cap \Delta) = f_x(\Omega) f_x(\Delta)$$

  Por outro lado, $f_x(X - \Omega) = 1$ se e somente se $x \in X - \Omega$, ou seja, $x \notin \Omega$, assim temos que $f_x(\Omega) = 0$.
  Então, $f_x(X - \Omega) = 1 + f_x(\Omega)$.
  Com isto, podemos concluir que f_x é um homomorfismo.

  Assim, sendo f uma aplicação de X sobre $\{0,1\}^{\mathcal{B}(X)}$, podemos afirmar que ele assume valores em $\mathcal{S}(\mathcal{B}(X))$, já que f_x é um homomorfismo para qualquer $x \in X$.

- *A aplicação f é injetiva;*
  Sejam x e y elementos distintos de X. Como X é Hausdorff, podemos encontrar um conjunto aberto O tal que $x \in O$ e $y \notin O$. Mas O é a união de conjuntos abertos básicos da base $\mathcal{B}(X)$. Portanto, existe um conjunto aberto-fechado $\Omega \in \mathcal{B}(X)$ tal que $x \in \Omega$ e $y \notin \Omega$.
  Logo temos que, $f_x(\Omega) = 1$ e $f_y(\Omega) = 0$, portanto $f_x \neq f_y$. Concluindo esta prova.

- *A aplicação f é sobrejetiva sobre $\mathcal{S}(\mathcal{B}(X))$;*
  Seja h um elemento de $\mathcal{S}(\mathcal{B}(X))$, ou seja, um homomorfismo de $\mathcal{B}(X)$ sobre $\{0,1\}$. O ultrafiltro em $\mathcal{B}(X)$ associado a h é

  $$\mathcal{U} = \{\Omega \in \mathcal{B}(X) : h(\Omega) = 1\} = h^{-1}\left[\{1\}\right].$$

  Uma vez que $\mathcal{U}$ tem a propriedade de interseção finita, os elementos de $\mathcal{U}$ são fechados e visto que X é um espaço topológico compacto. Podemos afirmar que a interseção de todos os elementos de $\mathcal{U}$ é não vazia. Sendo assim, seja x um elementos desta interseção.
  Para todo conjunto aberto-fechado $\Omega \in \mathcal{B}(X)$, temos que:

  1. Ou $\Omega \in \mathcal{U}$, o que significa que, $f_x(\Omega) = 1$ e $h(\Omega) = 1$;
  2. Ou senão, $\Omega \notin \mathcal{U}$. Neste caso $X - \Omega \in \mathcal{U}$, portanto, $f_x(\Omega) = 0$ e $h(\Omega) = 0$.

  Logo, para todo $\Omega \in \mathcal{B}(X)$, $f_x(\Omega) = h(\Omega)$.
  Portanto,

  $$h = f_x = f(x).$$

- *A aplicação f é contínua;*
  Seja G um conjunto aberto que pertence a base de subconjuntos abertos-fechados de $\mathcal{S}(\mathcal{B}(X))$. De acordo com lema 29, existe um único elemento $\Omega \in \mathcal{B}(X)$ tal que

  $$G = \{h \in \mathcal{S}(\mathcal{B}(X)) : h(\Omega) = 1\}.$$

  A imagem inversa de G sobre a aplicação f é

  $$\{x \in X : f_x \in G\} = \{x \in X : f_x(\Omega) = 1\} = \{x \in X : x \in \Omega\} = \Omega.$$

  Portanto, Ω é um subconjunto aberto de X.

- *A aplicação inversa f^{-1} é continua.*
  Seja Ω uma conjunto aberto básico no espaço X (ou seja, um elemento de $\mathcal{B}(X)$). Como f é uma bijeção, a imagem inversa de Ω sobre f^{-1} é sua imagem direta sobre f.

Assim, temos que $f[\Omega] = \{f_x : x \in \Omega\}$. Agora, temos que mostrar que este conjunto é um conjunto aberto no espaço $\mathcal{S}(\mathcal{B}(X))$.
Defina $V = \{h \in \mathcal{S}(\mathcal{B}(X)) : h(\Omega) = 1\}$.
O conjunto V é aberto (é ainda um conjunto aberto básico, segundo lema 29). Se mostrarmos que $f[\Omega] = V$, completaremos nossa prova.
Para cada $x \in \Omega$, temos $f_x(\Omega) = 1$ por definição de f_x, então $f_x \in V$.
Logo, $f[\Omega] \subseteq V$.
Todo $h \in V$ tem uma pré-imagem $y \in X$ sobre a bijeção f, digamos $h = f_y$. Como $h \in V$, temos que $h(\Omega) = f_y(\Omega) = 1$, então $y \in \Omega$ e $f_y = h \in f[\Omega]$.
Então, $V \subseteq f[\Omega]$.

Portanto, podemos afirmar que f é um homeomorfismo, consequentemente, concluímos a nossa demonstração. ∎

4 Lógica intuicionista

Como descrito na Seção 3, na lógica clássica afirmativas são ou falsas ou verdadeiras, uma vez que vale o princípio do terceiro excuído.

A lógica intuicionista abandona a ideia de verdade absoluta, e afirmativas são consideradas válidas se e somente se existe uma prova *construtiva* da mesma. Ou seja, o princípio do terceiro excluído não é mais uma *tautologia* uma vez que não existe um método construtivo único que prove *qualquer* proposição ou a sua negação.

No Exemplo 5, vimos que a fórmula $p \vee \neg p$ só pôde ser provada porque duplicamos o sucedente do seqüente. Desta forma, evitamos ter que dizer de imediato quem vale: p ou $\neg p$.

Para evitar que tenhamos esse tipo de escolha não construtiva em um sistema intuicionista, devemos restringir os seqüentes válidos àqueles que possuam *exatamente* uma fórmula como sucedente.[6] Desta forma, fica claro, por exemplo que no sistema **G** as regras de weakening e contraction não são válidas à direita. As regras de negação devem também ser ajustadas. A Figura 6 apresenta o sistema **Gi**, derivado do sistema **G** para a lógica intuicionista.

Como conseqüência da restrição sobre a forma do seqüente na lógica intuicionista, temos que os seguintes seqüentes clássicos não são prováveis em **Gi**:

$\vdash A \vee \neg A$	princípio do terceiro excluído
$\vdash \neg A \vee \neg\neg A$	princípio fraco do terceiro excluído
$\neg\neg A \vdash A$	lei de dupla negação
$\vdash (A \supset B) \vee (B \supset A)$	lei de Dummett
$\vdash ((A \supset B) \supset A) \supset A$	lei de Pierce
$\neg(\neg A \wedge \neg B) \vdash A \vee B$	

Esse último sequente indica que as famosas *relações de dualidade de"De Morgan"* não são válidas.

Para um matemático preocupado em provar um teorema, é importante a ideia de que toda afirmativa pode ser provada - verdadeira se uma prova é apresentada ou falsa se existe um contra-exemplo. Além disso, várias técnicas de demostração utilizam implicitamente o príncipio do meio excluído.

Vejamos os seguintes exemplos.

Teorema 35 *Existem dois números irracionais x e y tais que x^y é racional.*

[6] Existem sistemas intuicionistas em que sequentes podem ter mais de uma fórmula no sucedente (veja [23]). Mas analisar esse tipo de cálculo está fora do nosso objetivo.

$$\frac{}{A \vdash A}\ \mathit{Inicial}$$

$$\frac{}{\Gamma \vdash \top}\ \top R \qquad \frac{\Gamma_1 \vdash A \quad \Gamma_2 \vdash B}{\Gamma_1, \Gamma_2 \vdash A \wedge B}\ \wedge R$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}\ \supset R \qquad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg R$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee \mathit{R1} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee \mathit{R2}$$

$$\frac{}{\Gamma, \bot \vdash C}\ \bot L \qquad \frac{\Gamma_1 \vdash A}{\Gamma_1, \Gamma_2, \neg A \vdash C}\ \neg L$$

$$\frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge \mathit{L1} \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge \mathit{L2}$$

$$\frac{\Gamma_1, A \vdash C \quad \Gamma_2, B \vdash C}{\Gamma_1, \Gamma_2, A \vee B \vdash C}\ \vee L \qquad \frac{\Gamma_1 \vdash A \quad \Gamma_1, B \vdash C}{\Gamma_1, \Gamma_2, A \supset B \vdash C}\ \supset L$$

$$\frac{\Gamma \vdash C}{\Gamma, A \vdash C}\ \mathit{weak}\ L \qquad \frac{\Gamma, A, A \vdash C}{\Gamma, A \vdash C}\ \mathit{cont}\ L$$

$$\frac{\Gamma_1 \vdash A \quad A, \Gamma_2 \vdash C}{\Gamma_1, \Gamma_2 \vdash C}\ \mathit{Cut}$$

Figura 6: Regras do sistema **Gi**

Prova
Suponha que $2^{\sqrt{2}}$ é racional, então tomamos $x = \sqrt{2}$ e $y = \sqrt{2}$. Caso contrário, se $2^{\sqrt{2}}$ é irracional, tomamos $x = 2^{\sqrt{2}}$ e $y = \sqrt{2}$. ∎

Observe que não temos como saber qual dos casos realmente acontece, porque não se sabe se $2^{\sqrt{2}}$ é racional ou irracional. Mas o princípio do meio excluído nos garante que uma das opções ocorre e isso é bastante natural de se aceitar. Então, para o exemplo acima descrito, o problema se limita ao fato de que a prova apresentada não é construtiva.

Outro caso surge com a seguinte afirmativa.

Teorema 36 *Existem sete 7's consecutivos na representação decimal do número* π *.*

Bem, ou alguém algum dia chega à uma representação de π com um número de casas decimais grande o suficiente de modo a encontrar sete 7's consecutivos ou então não se sabe.

Esse é um exemplo de uma afirmativa para o qual não existe sentido a sua negação, uma vez que essa provavelmente nunca poderá ser provada. Ou seja, o princípio do meio excluído não se encaixa em um sistema que possui esse tipo de "teorema".

A lógica intuicionista abandona a ideia de verdade absoluta, e afirmativas são consideradas válidas se e somente se existem uma prova construtiva da mesma. Ou seja, o princípio do meio excluído não é mais válido.

4.1 Equivalência de sistemas

Implementar a lógica intuicionista é um pouquinho mais trabalhoso que a lógica clássica, por causa da regra de implicação à esquerda, como veremos a seguir.

Começamos por adaptar o sistema **Gi** para o caso de regras estruturais *weakening* e *contraction* implícitas, obtendo o sistema **G3i** da Figura 7.

Observe que a regra $\supset L$ explicitamente copia a fórmula $A \supset B$ da conclusão para a premissa da esquerda. Isso causa problemas seríssimos de implementação, uma vez que o interpretador poderá *sempre* escolher utilizar essa regra, entrando em *loop*.[7]

Desta forma, substituiremos a regra $\supset L$ de **G3i** (veja [6]) pelas quatro regras abaixo.

$$\frac{P, B, \Gamma \vdash E}{P, P \supset B, \Gamma \vdash E}\ L0\supset \qquad \frac{C \supset D \supset B, \Gamma \vdash E}{(C \wedge D) \supset B, \Gamma \vdash E}\ L\wedge\supset$$

$$\frac{C \supset B, D \supset B, \Gamma \vdash E}{(C \vee D) \supset B, \Gamma \vdash E}\ L\vee\supset \qquad \frac{C, D \supset B, \Gamma \vdash D \quad B, \Gamma \vdash E}{(C \supset D) \supset B, \Gamma \vdash E}\ L\supset\supset$$

onde P é atômico.

Obtendo assim o sistema **G3i′**. (Veja figura 8)

[7]Observe que a mesma discussão serve para a regra $\forall L$ de **G3** e **G3i** e $\exists R$ de **G3**. Mas como PLLIC implementa apenas a parte proposicional das lógicas em questão, nos limitaremos a discutir o problema da implicação.

$$\frac{}{\Gamma, A \vdash A}\ \textit{Inicial}$$

$$\frac{}{\Gamma \vdash \top}\ \top R \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge R$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}\ \supset R \qquad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg R$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee R1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee R2$$

$$\frac{\Gamma \vdash A[x/y]}{\Gamma \vdash \forall x A}\ \forall R \qquad \frac{\Gamma \vdash A[x/t]}{\Gamma \vdash \exists x A}\ \exists R$$

$$\frac{}{\Gamma, \bot \vdash C}\ \bot L \qquad \frac{\neg A, \Gamma \vdash A}{\Gamma, \neg A \vdash C}\ \neg L$$

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L$$

$$\frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ \vee L \qquad \frac{\Gamma, A \supset B \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \supset B \vdash C}\ \supset L$$

$$\frac{\Gamma, A[x/t], \forall x A \vdash C}{\Gamma, \forall x A \vdash C}\ \forall L \qquad \frac{\Gamma, A[x/y] \vdash C}{\Gamma, \exists x A \vdash C}\ \exists L$$

Figura 7: Sistema **G3i** para a lógica intuicionista de primeira ordem

Os sistemas lógicos **G3i′** e **G3i** são equivalentes. Mas para demonstramos esta equivalência necessitaremos do resultado expresso no lema a seguir.

Lema 37 $\Gamma, (C \supset D) \supset B \vdash C \supset D$ *é provável em G3i se e somente se* $\Gamma, D \supset B \vdash C \supset D$ *também possui prova em G3i.*

Prova
Aplicando às fórmulas $\Gamma, (C \supset D) \supset B \vdash C \supset D$ (Π_1) e $\Gamma, D \supset B \vdash C \supset D$ (Π_2) as regras dos sistema G3i, temos:

$$\dfrac{\dfrac{\overset{\pi_1}{\Gamma, (C \supset D) \supset B, C \vdash C \supset D} \quad \overset{\pi}{\Gamma, B, C \vdash D}}{\Gamma, (C \supset D) \supset B, C \vdash D} \supset L}{\underset{\Pi_1}{\Gamma, (C \supset D) \supset B \vdash C \supset D}} \supset R$$

e

$$\dfrac{\dfrac{\overset{\pi_2}{\Gamma, D \supset B, C \vdash D} \quad \overset{\pi}{\Gamma, B, C \vdash D}}{\Gamma, D \supset B, C \vdash D} \supset L}{\underset{\Pi 2}{\Gamma, D \supset B \vdash C \supset D}} \supset R$$

Assim podemos perceber que:

- Pela inversibilidade da regra $\supset R$, temos que Π_1 é verdadeiro se π_1 é provável. Que por sua vez é verdadeiro se e somente se, π também o for;
- Π_2 é provável se e somente se, π também o for.

Por tanto, para que Π_1 e Π_2 sejam prováveis basta π ser provável. Assim, Π_1 é provável se e só se Π_2 é provável.

∎

$$\frac{}{\Gamma, A \vdash A}\ Inicial$$

$$\frac{}{\Gamma \vdash \top}\ \top R \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge R$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}\ \supset R \qquad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg R$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee R1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee R2$$

$$\frac{\Gamma \vdash A[x/y]}{\Gamma \vdash \forall x A}\ \forall R \qquad \frac{\Gamma \vdash A[x/t]}{\Gamma \vdash \exists x A}\ \exists R$$

$$\frac{}{\Gamma, \bot \vdash C}\ \bot L \qquad \frac{\neg A, \Gamma \vdash A}{\Gamma, \neg A \vdash C}\ \neg L$$

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge L \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ \vee L$$

$$\frac{P, B, \Gamma \vdash E}{P, P \supset B, \Gamma \vdash E}\ L0 \supset \qquad \frac{C \supset D \supset B, \Gamma \vdash E}{(C \wedge D) \supset B, \Gamma \vdash E}\ L\wedge \supset$$

$$\frac{C \supset B, D \supset B, \Gamma \vdash E}{(C \vee D) \supset B, \Gamma \vdash E}\ L\vee \supset \qquad \frac{C, D \supset B, \Gamma \vdash D \quad B, \Gamma \vdash E}{(C \supset D) \supset B, \Gamma \vdash E}\ L \supset\supset$$

$$\frac{\Gamma, A[x/t], \forall x A \vdash C}{\Gamma, \forall x A \vdash C}\ \forall L \qquad \frac{\Gamma, A[x/y] \vdash C}{\Gamma, \exists x A \vdash C}\ \exists L$$

Figura 8: Sistema **G3i′** para a lógica intuicionista de primeira ordem

Teorema 38 *O sistema* **G3i′** *é equivalente ao sistema* **G3i**.

Prova

Note que as únicas regras que são distintas entre os dois sistemas (Veja figuras 7 e 8) são aquelas que envolvem a implicação do lado esquerdo da prova. Portanto, para mostrarmos a equivalência destes sistemas, basta ver que estas regras são equivalentes.

Primeiramente mostraremos que se um sequente $A \supset B, \Gamma \vdash \Delta$ é provável em $G3i$ ele também será provável em $G3i'$. Para isso, usaremos o método de indução sobre o ***tamanho da fórmula***[8] **principal**. Separemos, portanto, este problema em cinco casos, como veremos a seguir.

1.i $\mathbf{A = C \wedge D}$

Ou seja, $(C \wedge D) \supset B, \Gamma \vdash \Delta$ é provável em G3i. Note que $(C \wedge D) \supset B \equiv C \supset (D \supset B)$ em G3i. De fato, pois

$$\dfrac{\dfrac{\dfrac{\dfrac{C, D, C, (C \wedge D) \supset B \vdash C \quad C, C, D, (C \wedge D) \supset B \vdash D}{C, D, (C \wedge D) \supset B \vdash C \wedge D}\wedge R \qquad B \vdash B}{(C \wedge D) \supset B, C, D \vdash B}\supset L}{(C \wedge D) \supset B, C \vdash D \supset B}\supset R}{(C \wedge D) \supset B \vdash C \supset (D \supset B)}\supset R$$

e

$$\dfrac{\dfrac{\dfrac{C, D, C \supset (D \supset B) \vdash C \qquad \dfrac{D \supset B, C, D \vdash D \quad C, D, B \vdash B}{D \supset B, C, D \vdash B}\supset L}{C \supset (D \supset B), C, D \vdash B}\supset L}{C \supset (D \supset B), C \wedge D \vdash B}\wedge L}{C \supset (D \supset B) \vdash (C \wedge D) \supset B}\supset R$$

Já que, $(C \wedge D) \supset B, \Gamma \vdash \Delta$ é provável em G3i, pela equivalência acima, podemos concluir que $C \supset (D \supset B), \Gamma \vdash \Delta$ também é provável.

Como tamanho de A em $A \supset B$ é menor, pois agora $A = C$ e não mais $C \wedge D$, podemos aplicar a hipótese de indução.

Ou seja, $C \supset (D \supset B), \Gamma \vdash \Delta$ é provável em $G3i'$. Logo, pela regra $L\wedge \supset$

$$\dfrac{C \supset (D \supset B), \Gamma \vdash \Delta}{(C \wedge D) \supset B, \Gamma \vdash \Delta}L\wedge \supset$$

Concluimos que $(C \wedge D) \supset B, \Gamma \vdash \Delta$ é provável em $G3i'$.

[8] O tamanho de uma fórmula é medido pelo número de conectivos que esta fórmula possui.

1.ii $\mathbf{A} = \mathbf{C} \lor \mathbf{D}$
Por hipótese temos que $(C \lor D) \supset B, \Gamma \vdash \Delta$ é provável em G3i. Neste caso também recorreremos a uma equivalência para concluir a prova. Sabemos que $(C \lor D) \supset B \equiv (C \supset B) \land (D \supset B)$, pois

$$\dfrac{\dfrac{\dfrac{\dfrac{(C \lor D) \supset B, C \vdash C}{(C \lor D) \supset B, C \vdash C \lor D}\lor R1 \quad C, B \vdash B}{(C \lor D) \supset B, C \vdash B}\supset L}{(C \lor D) \supset B \vdash C \supset B}\supset R \quad \dfrac{\dfrac{\dfrac{(C \lor D) \supset B, D \vdash D}{(C \lor D) \supset B, D \vdash C \lor D}\lor R2 \quad D, B \vdash B}{(C \lor D) \supset B, D \vdash B}\supset L}{(C \lor D) \supset B \vdash D \supset B}\supset R}{(C \lor D) \supset B \vdash (C \supset B) \land (D \supset B)}\land R$$

e

$$\dfrac{\dfrac{\dfrac{\dfrac{C \supset B, D \supset B, C \vdash C \quad D \supset B, C, B \vdash B}{C \supset B, D \supset B, C \vdash}\supset L \quad \dfrac{C \supset B, D \supset B, D \vdash D \quad C \supset B, D \supset B, D, B \vdash B}{C \supset B, D \supset B, D \vdash B}\supset L}{C \supset B, D \supset B, C \lor D \vdash B}\lor L}{(C \supset B) \land (D \supset B), C \lor D \vdash B}\land L}{(C \supset B) \land (D \supset B) \vdash (C \lor D) \supset B}\supset R$$

Assim, temos que $(C \supset B) \land (D \supset B), \Gamma \vdash \Delta$ é provável em $G3i$. Pela regra $\land L$, vemos que $C \supset B, D \supset B, \Gamma \vdash \Delta$ também é provável. Logo, por hipótese de indução, temos que existe uma prova deste sequente em $G3i'$. Aplicando a regra $L\lor \supset$ temos que

$$\dfrac{C \supset B, D \supset B, \Gamma \vdash \Delta}{(C \lor D) \supset B, \Gamma \vdash \Delta}\, L\lor \supset$$

possui uma prova em $G3i'$.

1.iii $\mathbf{A} = \mathbf{C} \supset \mathbf{D}$
Ou seja, por hipótese $(C \supset D) \supset B, \Gamma \vdash \Delta$ possui um prova π em $G3i$ tal que π é da forma:

$$\dfrac{(C \supset D) \supset B, \Gamma \vdash C \supset D \quad B, \Gamma \vdash \Delta}{(C \supset D) \supset B, \Gamma \vdash \Delta}\supset L$$

Mas, pelo lema anterior, sabemos que $(C \supset D) \supset B, \Gamma \vdash C \supset D$ é provável em $G3i$ se, e somente se $D \supset B, \Gamma \vdash C \supset D$ também o é. Como o tamanho deste segundo sequente é menor que o tamanho do sequente $(C \supset D) \supset B, \Gamma \vdash C \supset D$ temos, por indução, que $D \supset B, \Gamma \vdash C \supset D$ possui um prova em $G3i'$. Logo pela regra $\supset R$,

$$\dfrac{C, D \supset B, \Gamma \vdash D}{D \supset B, \Gamma \vdash C \supset D}\supset R$$

temos que $C, D \supset B, \Gamma \vdash D$ é provável em $G3i'$

Da mesma maneira, temos que o tamanho do sequente $B, \Gamma \vdash \Delta$ é menor que o tamanho de nossa hipótese. Logo, por indução, ele também é provável em $G3i'$. Combinando estes sequentes com a regra $L \supset\supset$, concluimos que

$$\frac{C, D \supset B, \Gamma \vdash D \quad B, \Gamma \vdash \Delta}{(C \supset D) \supset B, \Gamma \vdash \Delta}\ L \supset\supset$$

é provável em $G3i'$.

1.iv **A é atômico**

Suponha que Γ contenha o par $A, A \supset B$, ou seja, $\Gamma = A, A \supset B, \Gamma'$.

Então por hipótese temos que $A, A \supset B, \Gamma' \vdash \Delta$ é provável em $G3i$. Pela regra $\supset L$,

$$\frac{A, A \supset B, \Gamma' \vdash \Delta, A \quad A, B, \Gamma' \vdash \Delta}{A, A \supset B, \Gamma' \vdash \Delta} \supset L$$

o sequente $A, B, \Gamma' \vdash \Delta$ possui prova em $G3i$. Consequentemente, por hipótese de indução, concluimos que existe uma prova de $A, B, \Gamma' \vdash \Delta$ em $G3i'$

Logo, aplicando a regra $L0 \supset$

$$\frac{A, B, \Gamma' \vdash \Delta}{A, A \supset B, \Gamma' \vdash \Delta}\ L0 \supset$$

é provável em $G3i'$.

1.v $\mathbf{A} = \bot$

Suponhamos que $A \supset B, \Gamma \vdash \Delta$ é provável em $G3i$. Como $\bot \supset B$ é sempre provável, podemos concluir que: $A \supset B, \Gamma \vdash \Delta$ se, e somente se, $\Gamma \vdash \Delta$ em $G3i$.

Assim, por hipótese de indução, $\Gamma \vdash \Delta$ possui uma prova em $G3i'$.

Sendo a regra *weakening* admissível em $G3i$, temos que

$$\frac{\Gamma \vdash \Delta}{A \supset B, \Gamma \vdash \Delta}\ weakL$$

ou seja, também existe uma prova em $G3i'$ de $A \supset B, \Gamma \vdash \Delta$.

Agora, mostraremos que as regras de implicação do sistema $G3i'$ podem ser simuladas pelo sistema lógico $G3i$. Ou seja, se existe uma prova em $G3i'$ para $A \supset B, \Gamma \vdash \Delta$, também existe uma prova em $G3i$.

2.i **L ⊃⊃**

Com o resultado obtido no lema anterior a este teorema, temos que $L\supset\supset = \supset L$ + Lema + $\supset R$. De fato,

$$\dfrac{C, D \supset B, \Gamma \vdash D \quad B, \Gamma \vdash \Delta}{(C \supset D) \supset B, \Gamma \vdash \Delta}\, L\supset\supset$$

$$\dfrac{\dfrac{\dfrac{C, D \supset B, \Gamma \vdash D}{D \supset B, \Gamma \vdash C \supset D}\supset R}{(C \supset D) \supset B, \Gamma \vdash C \supset B}\,Lema \quad B, \Gamma \vdash \Delta}{(C \supset D) \supset B, \Gamma \vdash \Delta}\supset L$$

2.ii **L∧ ⊃**

Supondo que $(C \wedge D) \supset B, \Gamma \vdash \Delta$ é provável em $G3i$, tem-se pela equivalência mostrada no caso 1.i que $C \supset D \supset B, \Gamma \vdash \Delta$ também possui prova em $G3i$. Ou seja,

$$\dfrac{C \supset D \supset B, \Gamma \vdash \Delta}{(C \wedge D) \supset B, \Gamma \vdash \Delta}\, L\wedge\supset \qquad \dfrac{C \supset D \supset B, \Gamma \vdash \Delta}{(C \wedge D) \supset B, \Gamma \vdash \Delta}\, Eq.1.i$$

temos que $L\wedge\supset$=Eq. 1.i

2.iii **L∨ ⊃**

Utilizando a equivalência demonstrada no caso 1.ii, mostraremos que $L\vee\supset$=Eq. 1.ii + $\wedge L$. Já que,

$$\dfrac{C \vee B, D \vee B, \Gamma \vdash \Delta}{(C \vee D) \supset B, \Gamma \vdash \Delta}\, L\vee\supset \qquad \dfrac{\dfrac{C \vee B, D \vee B, \Gamma \vdash \Delta}{(C \vee B) \wedge (D \vee B), \Gamma \vdash \Delta}\wedge L}{(C \vee D) \supset B, \Gamma \vdash \Delta}\, Eq.1.ii$$

2.iv **L0 ⊃**

Suponha que $P, P \supset B, \Gamma \vdash \Delta$ seja provável em $G3i$ com prova π, onde P é atômico e π é da forma:

$$\dfrac{\dfrac{}{P, P \supset B, \Gamma \vdash P}\,inicial \quad P, B, \Gamma \vdash \Delta}{P, P \supset B, \Gamma \vdash \Delta}\supset L$$

Portanto,

$$\dfrac{P, B, \Gamma \vdash \Delta}{P, P \supset B, \Gamma \vdash \Delta}\, L0\supset$$

pode ser simulada neste sistema.

Sendo assim, podemos concluir nossa demonstração.

∎

4.2 Especificando a lógica intuicionista

No sistema **G3i′** o problema de *loop* para o caso de implicação à esquerda foi resolvido. Porém, note que este mesmo problema ocorre na regra de negação à esquerda. Mas, podemos utilizar a equivalência $\neg A \equiv A \supset \bot$ em $G3i$ (portanto, válida em $G3i'$) para resolver o problema de *loop*.

$$\dfrac{\dfrac{\neg A, A \vdash A}{\neg A, A \vdash \bot}\ \neg L}{\neg A \vdash A \supset \bot}\ \supset R \qquad \dfrac{\dfrac{A \supset \bot, A \vdash A \quad A, \bot \vdash \bot}{A \supset \bot, A \vdash \bot}\ \supset L}{A \supset \bot \vdash \neg A}\ \neg R$$

Sendo assim, podemos substituir as regras de negação por regras de implicação.

Na figura 8 podemos perceber que as regras negação não foram retiradas do sistema $G3i'$, pois embora ela possua um problema computacional estas regras facilitam as provas de sequentes que possuem negação em seu contexto. Portanto, ela só será substituida na implimentação da lógica intuicionista.

Com isto, podemos então facilmente especificar a lógica intuicionista:

```
prova G A :- membro A G.
prova G C :- membro false G.
prova G true.

prova G (A and B) :- prova G A, prova G B.
prova G (A imp B) :- prova (A::G) B.
prova G (A or B) :- prova G A; prova G B.
prova G (neg A) :- prova G (A imp false).

prova G (forall A) :- pi x\(prova G (A x)).
prova G (exists A) :- prova G (A T).

prova G C :- memb_and_rest (A and B) G G1, prova (A ::(B :: G1)) C.
prova G C :- memb_and_rest (A or B) G G1, prova (A :: G1) C,
             prova (B :: G1) C.
prova G C :- memb_and_rest ((neg A) imp B) G G1,
             prova (((A imp false) imp B)::G1) C.
prova G C :- memb_and_rest (neg A) G G1, prova ((A imp false)::G1) C.

prova G C :- memb (forall A) G, prova ((A T)::G) C.
prova G C :- memb_and_rest (exists A) G G1,
             pi x\(prova ((A x)::G1) C).
```

```
prova G E :- memb_and_rest (P imp B) G G1, atomico P, membro P G1,
             prova (B::G1) E.
prova G E :- memb_and_rest ((C and D) imp B) G G1,
             prova ((C imp (D imp B))::G1) E.
prova G E :- memb_and_rest ((C or D) imp B) G G1,
             prova ((C imp B)::(D imp B)::G1) E.
prova G E :- memb_and_rest ((C imp D) imp B) G G1,
             prova (C::(D imp B)::G1) D, prova (B::G1) E.
```

4.3 Semântica

Iremos, agora, desenvolver uma semântica para a lógica intuicionista. Seja $\mathcal{P}$ o conjunto de todas as fórmulas proposicionais, seja $\Gamma \subseteq \mathcal{P}$ (em particular Γ pode ser vazio) e seja $\sim$ a seguinte relação de equivalência:

$$\varphi \sim \psi \text{ se, e somente se, } \Gamma \vdash \varphi \to \psi \text{ e } \Gamma \vdash \psi \to \varphi.$$

Seja $\mathcal{L}_\Gamma = \mathcal{P}/\sim\; = \{[\varphi]_\sim : \varphi \in \mathcal{P}\}$, e defina uma ordem parcial $\leq$ sobre $\mathcal{L}_\Gamma$ por:

$$[\varphi]_\sim \leq [\psi]_\sim \text{ se, e somente se, } \Gamma \vdash \varphi \to \psi.$$

O fato de $\sim$ ser uma relação de equivalência e $\leq$ ser uma ordem parcial bem definida é consequência da provabilidade das seguintes fórmulas:

- $\varphi \to \varphi$;
- $(\varphi \to \psi) \to ((\psi \to \vartheta) \to (\varphi \to \vartheta))$;

Podemos também definir as seguintes operações sobre $\mathcal{L}_\Gamma$:

$$\begin{aligned}
[\varphi]_\sim \cup [\psi]_\sim &= [\varphi \vee \psi]_\sim\,; \\
[\varphi]_\sim \cap [\psi]_\sim &= [\varphi \wedge \psi]_\sim\,; \\
-[\varphi]_\sim &= [\neg\varphi]_\sim.
\end{aligned}$$

Estas operações estão bem definidas, já que as seguintes fórmulas são prováveis:

- $(\varphi \to \varphi') \to ((\psi \to \psi') \to ((\varphi \vee \psi) \to (\varphi' \vee \psi')))$;
- $(\varphi \to \varphi') \to ((\psi \to \psi') \to ((\varphi \wedge \psi) \to (\varphi' \wedge \psi')))$.
- $(\varphi \to \varphi') \to (\neg\varphi' \to \neg\varphi)\,$;

Podemos ver que as operações $\cap$ e $\cup$ são respectivamente as operações **ínfimo** e **supremo** da relação $\leq$, e que as leis de distributividade

$$(a \cup b) \cap c = (a \cap c) \cup (b \cap c) \text{ e } (a \cap b) \cup c = (a \cup c) \cap (b \cup c)$$

são satisfeitas. E portanto, $\mathcal{L}_\Gamma$ é um reticulado distrubutivo.

A classe $[\bot]_\sim$ é o menor elemento 0 de $\mathcal{L}_\Gamma$, pois $\bot \to \varphi$ é provável, e $[\top]_\sim$, onde $\top = \bot \to \bot$, é o maior elemento 1. Temos $[\top]_\sim = \{\varphi : \Gamma \vdash \varphi\}$.

Entretanto, há uma dificuldade com a operação complemento pois temos que, $-a \cap a = [\bot]_\sim$ mas não necessariamente que $-a \cup a = [\top]_\sim$. O melhor que podemos afirmar é que $-a$ é o *maior elemento tal que* $-a \cap a = 0$, que chamamos de um ***pseudo-complemento***. Como a negação é um caso especial da implicação, a definição anterior pode ser generalizada. Um elemento c é chamado um ***pseudo-complemento relativo*** de a com respeito a b, se e somente se, c é o maior elemento tal que $a \cap c \leq b$. O pseudo-complemento relativo, se existe, é denotado por $a \Rightarrow b$.
Não é difícil de ver que em $\mathcal{L}_\Gamma$

$$[\varphi]_\sim \Rightarrow [\psi]_\sim = [\varphi \to \psi]_\sim.$$

4.3.1 Álgebra de Heyting

Definição 25 *Uma **álgebra de Heyting** é um sistema algébrico da forma* $\mathcal{H} = \langle H, \cup, \cap, \Rightarrow, -, 0, 1\rangle$, *que satisfaz as seguintes condições:*

1. $\cup, \cap$ *são associativos e comutativos;*
2. $(a \cup b) \cap c = (a \cap c) \cup (b \cap c)$ *e* $(a \cap b) \cup c = (a \cup c) \cap (b \cup c)$*;*
3. $a \cup 0 = a$ *e* $a \cap 1 = a$*;*
4. $a \cup a = a$*;*
5. $a \cap c \leq b$ *é equivalente a* $c \leq a \Rightarrow b$ *(onde* $a \leq b$ *representa* $a \cup b = b$*);*
6. $-a = a \Rightarrow 0$.

Estas condições nos permite dizer que $\mathcal{H}$ é um reticulado distributivo com zero e pseudo-complemento relativo definido por cada par de elementos. Em particular, cada álgebra Booleana é uma álgebra de Heyting com $a \Rightarrow b$ definido como $-a \cup b$. Um exemplo de que uma álgebra de Heyting que não é uma álgebra de Boole é a álgebra de conjuntos abertos de um espaço topológico, por exemplo a álgebra de subconjuntos abertos do plano Euclidiano $\mathbb{R}^2$.

Definição 26 *Seja* $\mathcal{H} = \langle H, \cup, \cap, \Rightarrow, -, 0, 1\rangle$ *uma álgebra de Heyting.*

1. *Uma **valoração v** em* $\mathcal{H}$ *é uma aplicação* $v : PV \to H$.

2. *Dado a valoração v em $\mathcal{H}$, defina a aplicação $[\![\bullet]\!]_v : \mathcal{P} \to H$ por:*

$$\begin{array}{rcl} [\![p]\!]_v & = & v(p)\texttt{, para } p \in PV \\ [\![\bot]\!]_v & = & 0 \\ [\![\varphi \vee \psi]\!]_v & = & [\![\varphi]\!]_v \cup [\![\psi]\!]_v \\ [\![\varphi \wedge \psi]\!]_v & = & [\![\varphi]\!]_v \cap [\![\psi]\!]_v \\ [\![\varphi \to \psi]\!]_v & = & [\![\varphi]\!]_v \Rightarrow [\![\psi]\!]_v \end{array}$$

Como usual, escrevemos $v(\varphi)$ no lugar de $[\![\varphi]\!]_v$.

Notação: Seja $\mathcal{H} = \langle H, \cup, \cap, \Rightarrow, -, 0, 1\rangle$ uma álgebra de Heyting. Escrevemos:

- $\mathcal{H}, v \models \varphi$, sempre que $v(\varphi) = 1$;
- $\mathcal{H} \models \varphi$, sempre que $\mathcal{H}, v \models \varphi$, para todo v;
- $\mathcal{H}, v \models \Gamma$, sempre que $\mathcal{H}, v \models \varphi$, para todo $\varphi \in \Gamma$;
- $\mathcal{H} \models \Gamma$, sempre que $\mathcal{H}, v \models \Gamma$, para todo v;
- $\models \varphi$, sempre que, $\mathcal{H}, v \models \varphi$, para todo H, v;
- $\Gamma \models \varphi$, se e somente se, para toda valoração v: $(v(\psi) = 1$ para todo $\psi \in \Gamma$ $) \Rightarrow v(\varphi) = 1$ e v relacionado com a álgebra de Heyting $\mathcal{H}$;
- Escrevemos $\Gamma \not\models \varphi$ se $\Gamma \models \varphi$ não for o caso.

Definição 27 .

- *Uma v que satisfaz a fórmula φ é chamada de **modelo** de φ.*
- *Uma valoração v que satisfaz um conjunto de formulas Γ é chamado de **modelo** de Γ.*

Apresentaremos agora o sistema de **Dedução Natural**, presente em várias lógicas, em particular na lógica intuicionista. Por ser um sistema mais simples, a demonstração do próximo teorema será facilitada. Pois a dedução natural permite, por meio de um pequeno número de regras de inferência, demonstrar a validade de uma infinidade de fórmulas e argumentos sem a necessidade de considerar os valores que cada fórmula ou subfórmula recebe. Veja figura 9.

Dizemos que fórmula φ tal que $\models \varphi$ é ***intuicionistamente válida*** ou é uma ***tautologia intuicionista***. Isto segue do seguinte teorema de completude cuja noção de teorema e tautologia coincidem no cálculo proposicional intuicionista.

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge i \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge e \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge e$$

$$\frac{\Gamma, B \vdash A}{\Gamma \vdash A \rightarrow B} \rightarrow i \quad \frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \rightarrow e$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A} \bot e \quad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A} RAA$$

Figura 9: Sistema de Dedução Natural para a lógica intuicionista proposicional

Este teorema diz que o modelo semântico baseado em álgebra de Heyting é completo (ou seja, que todos os argumentos semanticamente válidos também são sintaticamente válidos) e adequado (ou seja, que todos os argumentos sintaticamente válidos também são semanticamente válidos.):

Teorema 39 ***(Adequação e Completude)*** *As seguintes condições são equivalentes:*

1. $\Gamma \vdash \varphi$;
2. $\Gamma \models \varphi$.

Prova
(1) $\Rightarrow$ (2) : Adequação.
Sabemos que $\Gamma \vdash \varphi$ se e somemente se, existe uma derivação $\mathcal{D}$ com conclusão φ e com todas as hipóteses em Γ. Assim, é suficiente mostrar que, para cada derivação $\mathcal{D}$ com conclusão φ e hipóteses em Γ temos que $\Gamma \models \varphi$.
Para isto, usaremos indução em $\mathcal{D}$.

- **Caso Base**
  Suponhamos que a derivação $\mathcal{D}$ tenha apenas um elemento, evidentemente teremos que $\varphi \in \Gamma$. Ou seja,

  $$\frac{}{\Gamma', \varphi \vdash \varphi} \textit{Axioma}$$

  $$\text{onde } \Gamma = \Gamma' \cup \{\varphi\}$$

  Como todo modelo $\Gamma' \cap \{\varphi\}$ é em particular uma modelo de φ. Podemos concluir que:

  $$\frac{}{\Gamma', \varphi \models \varphi} \quad ou \quad seja, \quad \frac{}{\Gamma \models \varphi}$$

- **($\wedge$ i)** Introdução do $\wedge$.
  Suponha que existam derivações $\mathcal{D}$ e $\mathcal{D}'$, tais que $\Gamma \vdash \varphi$ e $\Gamma' \vdash \varphi'$ respectivamente. Por hipótese de indução temos que $\Gamma \models \varphi$ e $\Gamma' \models \varphi'$. Seja $\Gamma'' = \Gamma \cup \Gamma'$. Aplicando a regra de introdução do $\wedge$, temos

  $$\frac{\Gamma'' \vdash \varphi \quad \Gamma'' \vdash \varphi'}{\Gamma'' \vdash \varphi \wedge \varphi'} \wedge I$$

  Também temos que, $\Gamma'' \models \varphi$ e $\Gamma'' \models \varphi'$.
  Seja v um valoração tal que $v(\psi) = 1$ para todo $\psi \in \Gamma''$, então $v(\varphi) = v(\varphi') = 1$. Logo

  $$v(\varphi \wedge \varphi') = v(\varphi) \cup v(\varphi') = 1.$$

  Portanto, $\Gamma'' \models \varphi \wedge \varphi'$.

- **($\rightarrow i$)** Introdução do $\rightarrow$.
  Suponha que exista uma prova para $\Gamma \vdash \varphi \rightarrow \psi$, cuja a ultima regra aplicada foi a $(\rightarrow I)$.
  Então temos uma prova para $\Gamma, \varphi \vdash \psi$.
  Por hipótese de indução temos que $\Gamma' \models \psi$, onde $\Gamma' = \Gamma \cup \{\varphi\}$.
  Então v é uma valoração tal que, $v(\varphi) = 1$ e $v(\chi) = 1$ para todo $\chi \in \Gamma$ então $v(\psi) = 1$.
  Como $v(\varphi \rightarrow \psi) = v(\varphi) \Rightarrow v(\psi)$ a tabela da verdade nos mostra que $v(\varphi \rightarrow \psi) = 1$ se todas as proposições em Γ tem valor 1. Logo,

  $$\Gamma \models \varphi \rightarrow \psi$$

- **($\perp$ e)**
  Para todos os Γ que contém as hipóteses da derivação $\mathcal{D}$ com conclusão $\perp e$, temos por hipótese de indução que $\Gamma \models \perp$.
  Como $v(\perp) = 0$ para qualquer valoração. Não existe valoração, tal que $v(\psi) = 1$ em todos os $\psi \in \Gamma$.
  Assim, definindo $\Gamma' = \Gamma \cup \{\perp\}$. Suponha que $\Gamma' \not\models \varphi$, então para todo $\psi \in \Gamma$ tem-se $v(\psi) = 1$ e $v(\varphi) = 0$, para alguma valoração v. Uma contradição, já que $v(\perp) = 0$ para toda valoração. Logo,

  $$\Gamma' \models \varphi$$
  $$\Gamma, \perp \models \varphi$$

- **($\wedge$ e)** Exclusão do $\wedge$.
  Suponha que Γ contenha as hipóteses de derivação $\mathcal{D}$ com conclusão $\varphi \wedge \psi$. Ou seja, $\Gamma \vdash \varphi \wedge \psi$.
  Supondo que a ultima regra aplicada foi ($\wedge$ e), temos

$$\frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi} \wedge e \quad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi} \wedge e.$$

Considere que Γ contenha todas as hipóteses das derivações com conclusões φ e ψ. Por hipótese de indução temos que, $\Gamma \vDash \varphi \wedge \psi$. Então, seja v uma valoração tal que $v(\chi) = 1$ para todo $\chi \in \Gamma$ e $v(\varphi \wedge \psi) = 1$. Logo, $v(\varphi) = v(\psi) = 1$.
Sendo assim, podemos concluir que

$$\Gamma \vDash \varphi \qquad \Gamma \vDash \psi.$$

- **($\rightarrow$ e)**. Exclusão da $\rightarrow$.
  Supondo que existam derivações $\mathcal{D}$ e $\mathcal{D}'$ com conclusões $\varphi \rightarrow \psi$ e φ, respectivamente.
  Ou seja, $\Gamma \vdash \varphi \rightarrow \psi$ e $\Gamma \vdash \varphi$. Aplicando a regra ($\rightarrow$ e) temos,

  $$\frac{\Gamma \vdash \varphi \rightarrow \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi} \rightarrow e.$$

  Por hipóptese de indução podemos afirmar que,

  $$\Gamma \vDash \varphi \rightarrow \psi \text{ e } \Gamma \vDash \varphi.$$

  Por tanto, seja v uma valoração, tal que, $v(\chi) = 1$ para todo $\chi \in \Gamma$, $v(\varphi \rightarrow \psi) = 1$ e $v(\varphi) = 1$.
  Como, $1 = v(\varphi \rightarrow \psi) = v(\varphi) \Rightarrow v(\psi)$.
  Podemos concluir que $v(\psi) = 1$. Logo,

  $$\Gamma \vDash \psi.$$

- **(RAA)** Redução ao absurdo.
  Assumindo que existe uma prova para $\Gamma, \neg\varphi \vdash \bot$, cuja a ultima regra aplicada foi a (RAA). Aplicando esta regra concluimos que $\Gamma \vdash \varphi$.
  Por hipótese de indução sabemos que existe uma prova para $\Gamma' \vDash \bot$, onde $\Gamma' = \Gamma \cup \{\neg\varphi\}$.
  Suponha que $\Gamma \nvDash \varphi$, ou seja, existe uma valoração v, tal que, $v(\psi) = 1$ para todo $\psi \in \Gamma$ e $v(\varphi) = 0$. Portanto, $v(\neg\varphi) = 1$.
  Assim tem-se que $v(\psi) = 1$ para todo $\psi \in \Gamma'$. Impossível, pois $\Gamma' \vDash \bot$.
  Consequentemente,

  $$\Gamma \vDash \varphi.$$

(2) $\Rightarrow$ (1) : Completude.
A demonstração desta propriedade será feira por contraposição. Ou seja, mostraremos que

$$\Gamma \nvdash \varphi \Rightarrow \Gamma \nvDash \varphi.$$

Assumindo que $\Gamma \nvdash \varphi$, temos que existe uma valoração v tal que, $v(\psi) = 1$ para todo $\psi \in \Gamma$ e $v(\varphi) = 0$. Por tanto, pela definição temos que $\Gamma \nvDash \varphi$.

5 Lógica linear

Imagine uma situação real de descrever uma máquina de vender refrigerantes, não é adequado usar uma lógica de recursos infinitos. Ou seja, se uma latinha de guaraná custa um real e tenho um real na minha carteira, posso comprar apenas uma latinha e, no fim do processo, vou estar sem dinheiro.

A Lógica linear (desenvolvida por Girard [9]) lida com situações como essa: é uma lógica de *recursos conscientes*. Em Lógica linear, afirmativas não podem ser livremente copiadas (*Contraction*) ou descartadas (*Weakening*), apenas em situações especiais, onde aparece um tipo muito particular de conectivos: os exponenciais "?" e "!". Intuitivamente, $!B$ significa que o recurso B pode ser usado tantas vezes quanto necessárias. De maneira dual, $?B$ indica a possibilidade de produção de uma quantidade infinita da conclusão B.

A implicação linear é representada pelo símbolo "$\multimap$" e o significado de $A \multimap B$ é:

$$\text{consome-se } A \text{ dando origem a } B$$

Isto significa que, a partir do ponto em que B é produzido, o predicado A deixa de ser válido. A implicação intuicionista "$\Rightarrow$" então significa:

$$A \Rightarrow B \equiv\, !A \multimap B$$

ou seja, um predicado A implica B intuicionisticamente se e somente se existe uma quantidade infinita de A que linearmente implica B.

A ausência de *Contraction* e *Weakening* muda a natureza dos conectivos lógicos. De fato, a conjunção intuicionista (assim como a disjunção) é separada em dois conectivos diferentes. Portanto, existem duas maneiras distintas de formular a conjunção, correspondendo a dois conectivos distintos em Lógica Linear: o conectivo multiplicativo "$\otimes$" ($A \otimes B$ significa ambos A e B) e o aditivo "&" ($A \& B$ = escolha entre A e B). O mesmo para a disjunção: multiplicativo "$\parr$" ($A \parr B$ é igual a A paralelo a B) e aditivo "$\oplus$" ($A \oplus B$ significa ou A ou B).

Lógica Linear utiliza ainda os seguintes conectivos: $\bot$, e 1 para a versão multiplicativa de falso e verdadeiro respectivamente; 0, $\top$ para a versão aditiva desses conectivos; e $\forall$ e $\exists$ para quantificações universal e existencial. Veja a Figura 10 para o sistema de seqüentes da lógica linear.

5.1 Forum

Os conectivos lineares podem ser separados em dois grupos, *síncronos* e *assíncronos* [1], dependendo se a regra de introdução à direita para aquele conectivo depende ou não do seu contexto.

Axioma e regras Cut

$$\frac{}{A \vdash A}\ initial \qquad \frac{\Gamma_1 \vdash \Delta_1, A \quad A, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ Cut$$

$$\frac{\Gamma_1 \vdash \Delta_1, !\,A \quad (!\,A)^n, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ Cut! \qquad \frac{\Gamma_1 \vdash \Delta_1, (?\,A)^n \quad ?\,A, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ Cut?$$

Regras à direita

$$\frac{}{\Gamma \vdash \top, \Delta}\ \top R \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \bot, \Delta}\ \bot R \qquad \frac{}{\vdash 1}\ 1R$$

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \,\&\, B, \Delta}\ \& R \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \parr B, \Delta}\ \parr R$$

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \oplus B, \Delta}\ \oplus R_1 \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \oplus B, \Delta}\ \oplus R_2$$

$$\frac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash A \otimes B, \Delta_1, \Delta_2}\ \otimes R \qquad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \multimap B, \Delta}\ \multimap R$$

$$\frac{\Gamma \vdash A[x/y], \Delta}{\Gamma \vdash \forall x A, \Delta}\ \forall R \qquad \frac{\Gamma \vdash A[x/t], \Delta}{\Gamma \vdash \exists x A, \Delta}\ \exists R$$

Regras à esquerda

$$\frac{}{0, \Gamma \vdash \Delta}\ 0L \qquad \frac{}{\bot \vdash}\ \bot L \qquad \frac{\Gamma \vdash \Delta}{1, \Gamma \vdash \Delta}\ 1L$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \,\&\, B \vdash \Delta}\ \& L_1 \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \,\&\, B \vdash \Delta}\ \& L_2$$

$$\frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \oplus B \vdash \Delta}\ \oplus L \qquad \frac{\Gamma_1, A \vdash \Delta_1 \quad \Gamma_2, B \vdash \Delta_2}{\Gamma_1, \Gamma_2, A \parr B \vdash \Delta_1, \Delta_2}\ \parr L$$

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \otimes B \vdash \Delta}\ \otimes L \qquad \frac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2, B \vdash \Delta_2}{\Gamma_1, \Gamma_2, A \multimap B \vdash \Delta_1, \Delta_2}\ \multimap L$$

$$\frac{\Gamma, A[x/t] \vdash \Delta}{\Gamma, \forall x A \vdash \Delta}\ \forall L \qquad \frac{\Gamma, A[x/y] \vdash \Delta}{\Gamma, \exists x A \vdash \Delta}\ \exists L$$

Exponenciais

$$\frac{\Gamma \vdash \Delta}{\Gamma, !\,A \vdash \Delta}\ !\,W \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma, !\,A \vdash \Delta}\ !\,L \qquad \frac{\Gamma, !\,A, !\,A \vdash \Delta}{\Gamma, !\,A \vdash \Delta}\ !\,C \qquad \frac{!\,\Gamma \vdash A, ?\,\Delta}{!\,\Gamma \vdash !\,A, ?\,\Delta}\ !\,R$$

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash ?\,A, \Delta}\ ?\,W \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma \vdash ?\,A, \Delta}\ ?\,R \qquad \frac{\Gamma \vdash ?\,A, ?\,A, \Delta}{\Gamma \vdash ?\,A, \Delta}\ ?\,C \qquad \frac{!\,\Gamma, A \vdash ?\,\Delta}{!\,\Gamma, ?\,A \vdash ?\,\Delta}\ ?\,L$$

Figura 10: Cálculo LL para a lógica linear

Podemos notar pelas regras à direita da figura 10 que os conectivos síncronos são 1, $\otimes$, $\oplus$, 0, !, $\exists$ e os assíncronos são ?, $\parr$, $\perp$, &, $\top$, $\multimap$, e $\forall$.

Uma outra característica que diferencia os conectivos síncronos dos assíncronos diz respeito a inversibilidade das regras de inferência. A conclusão de um regra de inferência associada a um conectivo assíncrono é derivável [9] se e somente se todas as premissas são deriváveis. Esta propriedade não está presente nos conectivos síncronos.

O *de Morgan dual* de um conectivo em uma dessas classes é um conectivo na outra classe. Ou seja, o dual de um conectivo síncrono é um conectivo assíncrono e vice-versa.

Dada essa divisão de conectivos, Miller propôs em [16] a presentação *Forum* de lógica linear na qual fórmulas são construídas utilizando apenas os conectivos assíncronos junto com a versão intuicionista da implicação $B \Rightarrow C$ ($B \Rightarrow C$ denota $!\, B \multimap C$).[10] Os conectivos síncronos da lógica linear estão disponíveis implicitamente, uma vez que conectivos que aparecem no lado esquerdo do seqüente comportam-se de modo síncrono.

O objetivo de apresentar *Forum* é que este possui um algoritmo de prova de seqüentes: a busca por provas em seqüentes com conectivos assíncronos no sucedente corresponde à busca *goal directed*, enquanto que conectivos assíncronos no antecedente correspondem ao procedimento de *backchaining* sobre cláusulas de programas [15].

Ao mesmo tempo, Forum captura toda a lógica linear, uma vez que os conectivos que faltam podem ser definidos utilizando as seguintes equivalências lógicas:

$$\begin{array}{cccc} B^\perp \equiv B \multimap \perp & 0 \equiv \top \multimap \perp & 1 \equiv \perp \multimap \perp & \exists x.B \equiv (\forall x.B^\perp)^\perp \\ !\, B \equiv (B \Rightarrow \perp) \multimap \perp & B \oplus C \equiv (B^\perp \,\&\, C^\perp)^\perp & & B \otimes C \equiv (B^\perp \parr C^\perp)^\perp \end{array}$$

Antes de demonstrarmos estas equivalências chamaremos a atenção para o fato de que $(\ \vdash B^\perp) \equiv (B \vdash\ )$ e $(B^\perp \vdash\ ) \equiv (\ \vdash B)$.

Sendo assim, denotaremos por $\perp$ o uso desta propriedade durante a prova das equivalências.

- $B^\perp \equiv B \multimap \perp$

[9] Uma regra derivável é aquela em que a conclusão pode ser originada de suas premissas usando outras regras.

[10] Utilizamos aqui o símbolo $\Rightarrow$ ao invés de $\supset$ por uma questão de didática: queremos separar completamente as lógicas dadas por **G** da lógica *LL*.

$$
\dfrac{\dfrac{\dfrac{B \vdash B}{B \vdash B, \bot}\ \bot R}{\vdash B \multimap \bot, B}\ \multimap R}{B^{\bot} \vdash B \multimap \bot}
\qquad
\dfrac{\dfrac{B \vdash B \qquad \dfrac{}{\bot \vdash}\ \bot L}{B, B \multimap \bot \vdash}\ \multimap L}{B \multimap \bot \vdash B^{\bot}}
$$

- $0 \equiv \top \multimap \bot$

$$
\dfrac{\dfrac{}{0, \top \vdash \bot}\ 0L}{0 \vdash \top \multimap \bot}\ \multimap R
\qquad
\dfrac{\dfrac{}{\vdash 0, \top}\ \top R \qquad \dfrac{}{\bot \vdash}\ \bot L}{\top \multimap \bot \vdash 0}\ \multimap L
$$

- $1 \equiv \bot \multimap \bot$

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\bot \vdash}\ \bot L}{1, \bot \vdash}\ 1L}{1, \bot \vdash \bot}\ \bot R}{1 \vdash \bot \multimap \bot}\ \multimap R
\qquad
\dfrac{\dfrac{}{\bot \vdash}\ \bot L \qquad \dfrac{\dfrac{}{\vdash 1}\ 1R}{\vdash 1, \bot}\ \bot R}{\bot \multimap \bot \vdash 1}\ \multimap L
$$

- $\exists x.B \equiv (\forall x.B^{\bot})^{\bot}$

$$
\dfrac{\dfrac{\dfrac{\dfrac{B(x) \vdash B(t)}{B(x), B^{\bot}(t) \vdash}}{\exists x.B, B^{\bot}(t) \vdash}\ \exists L}{\exists x.B, \forall x.B^{\bot} \vdash}\ \forall L}{\exists x.B \vdash (\forall x.B^{\bot})^{\bot}}
\qquad
\dfrac{\dfrac{\dfrac{\dfrac{B(x) \vdash B(t)}{\vdash B(t), B^{\bot}(x)}}{\vdash \exists x.B, B^{\bot}(x)}\ \exists L}{\vdash \exists x.B, \forall x.B^{\bot}}\ \forall R}{(\forall x.B^{\bot})^{\bot} \vdash \exists x.B}
$$

- $!\,B \equiv (B \Rightarrow \bot) \multimap \bot$

  Pela definição de $\Rightarrow$ vista no início desta seção, podemos reescrever esta equivalência como $!\,B \equiv (!\,B \multimap \bot) \multimap \bot$, assim

$$\dfrac{\dfrac{\bot \vdash \bot \qquad !\,B \vdash !\,B}{!\,B, B \multimap \bot \vdash \bot}\;\multimap L}{!\,B \vdash (!\,B \multimap \bot) \multimap \bot}\;\multimap R \qquad\qquad \dfrac{\bot \vdash \qquad \dfrac{\dfrac{!\,B \vdash !\,B}{!\,B \vdash !\,B, \bot}\;\bot R}{\vdash !\,B, !\,B \multimap \bot}\;\multimap R}{(!\,B \multimap \bot \vdash !\,B}\;\multimap L$$

- $B \oplus C \equiv (B^{\bot} \,\&\, C^{\bot})^{\bot}$

$$\dfrac{\dfrac{\dfrac{\dfrac{B \vdash B}{B, B^{\bot} \vdash}}{B, B^{\bot} \,\&\, C^{\bot} \vdash}\;\&L_1 \qquad \dfrac{\dfrac{C \vdash C}{C, C^{\bot} \vdash}}{C, B^{\bot} \,\&\, C^{\bot} \vdash}\;\&L_2}{B \oplus C, B^{\bot} \,\&\, C^{\bot} \vdash}\;\oplus L}{B \oplus C \vdash (B^{\bot} \,\&\, C^{\bot})^{\bot}}$$

$$\dfrac{\dfrac{\dfrac{B \vdash B}{\vdash B^{\bot}, B \oplus C}\;\oplus R_1 \qquad \dfrac{C \vdash C}{\vdash C^{\bot}, B \oplus C}\;\oplus R_2}{\vdash B \oplus C, B^{\bot} \,\&\, C^{\bot}}\;\&R}{(B^{\bot} \,\&\, C^{\bot})^{\bot} \vdash B \oplus C}$$

- $B \otimes C \equiv (B^{\bot} \parr C^{\bot})^{\bot}$

$$\dfrac{\dfrac{\dfrac{\dfrac{B \vdash B}{B, B^{\bot} \vdash} \qquad \dfrac{C \vdash C}{C, C^{\bot} \vdash}}{B, C, B^{\bot} \parr C^{\bot} \vdash}\;\parr L}{B \otimes C, B^{\bot} \parr C^{\bot} \vdash}\;\otimes L}{B \otimes C \vdash (B^{\bot} \parr C^{\bot})^{\bot}} \qquad\qquad \dfrac{\dfrac{\dfrac{\dfrac{B \vdash B}{\vdash B^{\bot}, B} \qquad \dfrac{C \vdash C}{\vdash C^{\bot}, C}}{\vdash B^{\bot}, C^{\bot}, B \otimes C}\;\otimes R}{\vdash B^{\bot} \parr C^{\bot}, B \otimes C}\;\parr R}{(B^{\bot} \parr C^{\bot})^{\bot} \vdash B \otimes C}$$

É interessante observar que o sistema de provas de Forum que é dada na Figura 11, não é minimal. Pois, por exemplo, os conectivos $\parr$ e $?$ podem ser definidos em termos dos conectivos remanecentes.

De fato, $?\,B \equiv (B \multimap \bot) \Rightarrow \bot$ e $B \parr C \equiv (B \multimap \bot) \multimap C$. Já que:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{B \vdash B \quad \bot \vdash \bot}{B, B \multimap \bot \vdash \bot}\multimap L}{?\,B, B \multimap \bot \vdash \bot}\,?\,L}{?\,B, !(B \multimap \bot) \vdash \bot}\,!\,L}{?\,B \vdash !(B \multimap \bot) \multimap \bot}\multimap R}{?\,B \vdash (B \multimap \bot) \Rightarrow \bot} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{B \vdash B}{B \vdash \bot, B}\bot R}{\vdash B \multimap \bot, B}\multimap R}{\vdash !(B \multimap \bot), B}\,!\,R \quad \bot \vdash}{!(B \multimap \bot) \multimap \bot \vdash B}\multimap L}{!(B \multimap \bot) \multimap \bot \vdash ?\,B}\,?\,R}{(B \multimap \bot) \Rightarrow \bot \vdash ?\,B}$$

e

$$\dfrac{\dfrac{\dfrac{B \vdash B \quad \bot \vdash}{B, B \multimap \bot \vdash}\multimap L \qquad C \vdash C}{b \parr C, B \multimap \bot \vdash C}\parr L}{B \parr C \vdash (B \multimap \bot) \multimap C}\multimap R \qquad \dfrac{\dfrac{\dfrac{\dfrac{B \vdash B}{B \vdash \bot, B}\bot R}{\vdash B \multimap \bot, B}\multimap R \qquad C \vdash C}{(B \multimap \bot) \multimap C \vdash B, C}\multimap L}{(B \multimap \bot) \multimap C \vdash B \parr C}\parr R$$

Portanto, o número de conectivos no Forum poderia (caso necessário) ser ainda mais reduzido.

Seqüentes em Forum possuem uma das formas

$$\Sigma \colon \Psi; \Delta \longrightarrow \Gamma; \Upsilon \quad \text{e} \quad \Sigma \colon \Psi; \Delta \xrightarrow{B} \Gamma; \Upsilon,$$

onde Σ é uma assinatura, Δ e Γ são multiconjuntos de fórmulas, Ψ e Υ são conjuntos de fórmulas, e B é uma fórmula. Todas as fórmulas nos seqüentes são compostas dos conectivos assíncronos listados anteriormente (juntamente com $\Rightarrow$). Os significados de tais seqüentes em lógica linear são

$$!\,\Psi, \Delta \vdash \Gamma, ?\,\Upsilon \quad \text{e} \quad !\,\Psi, \Delta, B \vdash \Gamma, ?\,\Upsilon,$$

respectivamente.

No sistema de provas da Figura 11, as regras à direita atuam apenas sobre seqüentes da forma $\Sigma \colon \Psi; \Delta \longrightarrow \Gamma; \Upsilon$. A variável sintática $\mathcal{A}$ na Figura 11 denota um multiconjunto de fórmulas atômicas. Regras à esquerda são aplicadas apenas à fórmula B, que é o label de $\Sigma \colon \Psi; \Delta \xrightarrow{B} \mathcal{A}; \Upsilon$.

$$\frac{}{\Sigma\colon \Psi; \Delta \longrightarrow \top, \Gamma; \Upsilon}\ \top R$$

$$\frac{\Sigma\colon \Psi; \Delta \longrightarrow B, \Gamma; \Upsilon \quad \Sigma\colon \Psi; \Delta \longrightarrow C, \Gamma; \Upsilon}{\Sigma\colon \Psi; \Delta \longrightarrow B \,\&\, C, \Gamma; \Upsilon}\ \& R$$

$$\frac{\Sigma\colon \Psi; \Delta \longrightarrow \Gamma; \Upsilon}{\Sigma\colon \Psi; \Delta \longrightarrow \bot, \Gamma; \Upsilon}\ \bot R \qquad \frac{\Sigma\colon \Psi; \Delta \longrightarrow B, C, \Gamma; \Upsilon}{\Sigma\colon \Psi; \Delta \longrightarrow B \parr C, \Gamma; \Upsilon}\ \parr R$$

$$\frac{\Sigma\colon \Psi; B, \Delta \longrightarrow C, \Gamma; \Upsilon}{\Sigma\colon \Psi; \Delta \longrightarrow B \multimap C, \Gamma; \Upsilon}\ \multimap R \qquad \frac{\Sigma\colon B, \Psi; \Delta \longrightarrow C, \Gamma; \Upsilon}{\Sigma\colon \Psi; \Delta \longrightarrow B \Rightarrow C, \Gamma; \Upsilon}\ \Rightarrow R$$

$$\frac{y\colon \tau, \Sigma\colon \Psi; \Delta \longrightarrow B[y/x], \Gamma; \Upsilon}{\Sigma\colon \Psi; \Delta \longrightarrow \forall_\tau x.B, \Gamma; \Upsilon}\ \forall R \qquad \frac{\Sigma\colon \Psi; \Delta \longrightarrow \Gamma; B, \Upsilon}{\Sigma\colon \Psi; \Delta \longrightarrow ?\,B, \Gamma; \Upsilon}\ ?\,R$$

$$\frac{\Sigma\colon B, \Psi; \Delta \xrightarrow{B} \mathcal{A}; \Upsilon}{\Sigma\colon B, \Psi; \Delta \longrightarrow \mathcal{A}; \Upsilon}\ \mathit{decide}\,! \qquad \frac{\Sigma\colon \Psi; \Delta \longrightarrow \mathcal{A}, B; B, \Upsilon}{\Sigma\colon \Psi; \Delta \longrightarrow \mathcal{A}; B, \Upsilon}\ \mathit{decide}\,?$$

$$\frac{\Sigma\colon \Psi; \Delta \xrightarrow{B} \mathcal{A}; \Upsilon}{\Sigma\colon \Psi; B, \Delta \longrightarrow \mathcal{A}; \Upsilon}\ \mathit{decide}$$

$$\frac{}{\Sigma\colon \Psi; \cdot \xrightarrow{A} A; \Upsilon}\ \mathit{initial} \qquad \frac{}{\Sigma\colon \Psi; \cdot \xrightarrow{A} \cdot; A, \Upsilon}\ \mathit{initial}?$$

$$\frac{}{\Sigma\colon \Psi; \cdot \xrightarrow{\bot} \cdot; \Upsilon}\ \bot L \qquad \frac{\Sigma\colon \Psi; \Delta \xrightarrow{B_i} \mathcal{A}; \Upsilon}{\Sigma\colon \Psi; \Delta \xrightarrow{B_1 \& B_2} \mathcal{A}; \Upsilon}\ \& L_i \qquad \frac{\Sigma\colon \Psi; B \longrightarrow \cdot; \Upsilon}{\Sigma\colon \Psi; \cdot \xrightarrow{?\,B} \cdot; \Upsilon}\ ?\,\mathrm{L}$$

$$\frac{\Sigma\colon \Psi; \Delta_1 \xrightarrow{B} \mathcal{A}_1; \Upsilon \quad \Sigma\colon \Psi; \Delta_2 \xrightarrow{C} \mathcal{A}_2; \Upsilon}{\Sigma\colon \Psi; \Delta_1, \Delta_2 \xrightarrow{B \parr C} \mathcal{A}_1, \mathcal{A}_2; \Upsilon}\ \parr L \qquad \frac{\Sigma\colon \Psi; \Delta \xrightarrow{B[t/x]} \mathcal{A}; \Upsilon}{\Sigma\colon \Psi; \Delta \xrightarrow{\forall_\tau x.B} \mathcal{A}; \Upsilon}\ \forall L$$

$$\frac{\Sigma\colon \Psi; \Delta_1 \longrightarrow \mathcal{A}_1, B; \Upsilon \quad \Sigma\colon \Psi; \Delta_2 \xrightarrow{C} \mathcal{A}_2; \Upsilon}{\Sigma\colon \Psi; \Delta_1, \Delta_2 \xrightarrow{B \multimap C} \mathcal{A}_1, \mathcal{A}_2; \Upsilon}\ \multimap L$$

$$\frac{\Sigma\colon \Psi; \cdot \longrightarrow B; \Upsilon \quad \Sigma\colon \Psi; \Delta \xrightarrow{C} \mathcal{A}; \Upsilon}{\Sigma\colon \Psi; \Delta \xrightarrow{B \Rightarrow C} \mathcal{A}; \Upsilon}\ \Rightarrow L$$

Figura 11: Sistema de provas de Forum

5.2 Especificando a lógica linear

Epecificamos, na verdade, Forum. Como a busca por provas é *uniforme*, podemos sempre começar pelo sucedente, passando ao antecedente apenas quando temos apenas átomos do lado direito do seqüente.

```
rproof Psi Delta Atomos (top::Gama) Upsilon.

rproof Psi Delta Atomos ((B land C)::Gama) Upsilon :-
    rproof Psi Delta Atomos (B::Gama) Upsilon,
    rproof Psi Delta Atomos (C::Gama) Upsilon.
rproof Psi Delta Atomos ((B cimp C)::Gama) Upsilon :-
    rproof (B::Psi) Delta Atomos (C::Gama) Upsilon.
rproof Psi Delta Atomos (falso::Gama) Upsilon :-
    rproof Psi Delta Atomos Gama Upsilon.
rproof Psi Delta Atomos ((B lpar C)::Gama) Upsilon :-
    rproof Psi Delta Atomos (B::C::Gama) Upsilon.
rproof Psi Delta Atomos ((B limp C)::Gama) Upsilon :-
    rproof Psi (B::Delta) Atomos (C::Gama) Upsilon.
rproof Psi Delta Atomos ((? B)::Gama) Upsilon :-
    rproof Psi Delta Atomos Gama (B::Upsilon).


rproof Psi Delta Atomos (A::Gama) Upsilon:-
    atomic A, rproof Psi Delta (A::Atomos) Gama Upsilon.

rproof Psi Delta Atomos nil Upsilon:- memb_and_rest B Delta Delta1,
    lproof Psi Delta1 B Atomos Upsilon; memb B Psi,
    lproof Psi Delta B Atomos Upsilon; memb B Upsilon,
    rproof Psi Delta Atomos (B::nil) Upsilon.

lproof Psi nil A nil (A::Upsilon).
lproof Psi nil A (A::nil) Upsilon.
lproof Psi nil falso nil Upsilon.

lproof Psi Delta (B land C) Atomos Upsilon :-
    lproof Psi Delta B Atomos Upsilon;
    lproof Psi Delta C Atomos Upsilon.

lproof Psi Delta (B cimp C) Atomos Upsilon :-
    rproof Psi nil nil (B::nil) Upsilon,
    lproof Psi Delta C Atomos Upsilon.
```

```
lproof Psi nil (? B) nil Upsilon :-
    rproof Psi (B::nil) nil nil Upsilon.
lproof Psi Delta (B lpar C) Atomos Upsilon:-
    split Delta Delta1 Delta2, split Atomos Atomos1 Atomos2,
    lproof Psi Delta1 B Atomos1 Upsilon,
    lproof Psi Delta2 C Atomos2 Upsilon.
lproof Psi Delta (B limp C) Atomos Upsilon:-
    split Delta Delta1 Delta2, split Atomos Atomos1 Atomos2,
    rproof Psi Delta1 (B::Atomos1) Upsilon,
    lproof Psi Delta2 C Atomos2 Upsilon.

prova Psi Delta Gama Upsilon :- rproof Psi Delta nil Gama Upsilon.
```

6 Considerações Finais

Como visto na Seção 3, matemáticos começam de um conjunto de axiomas, provam alguns lemas e então as utilizam para provar teoremas. Algumas das provas utilizadas não são construtivas, e o uso da estratégia conhecida como *redução ao absurdo* é muito comum.

Uma vez que um lema é provado, ele pode ser usado de novo para provar outras proposições ou teoremas: um lema provado verdadeiro será verdadeiro para sempre. Portanto, matemáticos trabalham com a lógica clássica, a lógica da *verdade estável* e de *recursos e conclusões infinitos*.

A lógica intuicionista (Seção 4) joga fora essa noção de verdade absoluta e a veracidade de uma afirmativa depende da existência de uma prova (ou construção) da afirmativa.

Mas ainda, a lógica intuicionista é uma lógica de *infinitos recursos* – mas não infinitas conclusões, uma vez que permitir a prova de todos os resultados possíveis implica em permitir o princípio do terceiro excluído.

Já a lógica linear (Seção 5) é um refinamento da lógica clássica e intuicionista. Em vez de enfatizar a verdade, como na lógica clássica, ou a prova, como na lógica intuicionista, a lógica linear enfatiza o papel de fórmulas como recursos. Para atingir este foco, a lógica linear não permite que as regras usuais de contração estrutural e enfraquecimento aplicadas a todas as fórmulas, mas apenas aquelas fórmulas marcados com certos verbos modais.

Vimos que a lógica clássica é a lógica que corresponde naturalmente à classe das álgebras de Boole. Apresentamos um resultado muito conhecido de Stone que mostra que toda álgebra booleana finita é isomorfa á álgebra booleana de todos os subconjuntos de algum conjunto finito X.

Já na lógica intuicionista podemos estabelecer uma conexão entre a lógica e a álgebra de Heyting, e conhecemos o teorema de adequação e completude que nos permite estabelecer um equivalência entre a sintaxe e a semântica ao afirmarmos que teoremas são equivalentes a tautologias.

E através da construção de sistemas de provas (G3c, G3i' e Forum) para as três lógicas, podemos especifica-lás. E assim construir um provador lógico totalmente automático para estas três lógicas, nomeado PLLIC.

A Programas utilizados no PLLIC em λ-Prolog

```
module conectivos.

nao_atomico (A imp B).
nao_atomico (A and B).
nao_atomico (A or B).
nao_atomico false.
nao_atomico true.
nao_atomico (neg A).
nao_atomico one.
nao_atomico zero.
nao_atomico (A land B).
nao_atomico (A cimp B).
nao_atomico (A limp B).
nao_atomico (A lpar B).
nao_atomico (? A).
nao_atomico (bang A).
nao_atomico (A multand B).
nao_atomico (A addor B).

atomico B :- not (nao_atomico B).

expand zero (neg true).
expand one (neg false).
expand (bang A) (neg (A cimp false)).
expand (A addor B) (neg ((neg A) land (neg B))).
expand (A multand B) (neg ((neg A) lpar (neg B))).
expand (A limp B)  (A1 limp B1) :- expand A A1, expand B B1.
expand (A land B)  (A1 land B1) :- expand A A1, expand B B1.
expand (A lpar B)  (A1 lpar B1) :- expand A A1, expand B B1.
expand (? A)  (? A1) :- expand A A1.
expand (neg A)  (neg A1) :- expand A A1.
expand A A.
```

Figura 12: Módulo conectivos

```
sig conectivos.

kind form type.

type imp              form -> form -> form.    % implicacao intuicionista/classica
type and              form -> form -> form.    % conjuncao intuicionista/classica
type or               form -> form -> form.    % disjuncao intuicionista/classica
type false            form.                    % falso intuicionista/classico/ll
type true             form.                    % verdadeiro intuicionista/classico/ll
type neg              form -> form.            % negacao intuicionista/classica/linear
type limp             form -> form -> form.    % implicacao linear
type cimp             form -> form -> form.    % implicacao intuitionistica
type land             form -> form -> form.    % conjuncao linear aditiva
type lpar             form -> form -> form.    % disjuncao linear multiplicativa
type ?                form -> form.            % modal ?
type bang        form -> form. % modal !
type multand        form -> form -> form.    % conjuncao linear multiplicativa
type addor        form -> form -> form.    % disjuncao linear aditiva
type one              form.                    % verdadeiro linear aditivo
type zero             form.                    % falso linear aditivo

infixr  and   120.
infixr  or    120.
infixr  imp   110.
infixr land 2.
infixr multand 2.
infixr lpar 3.
infixr addor 3.
infixr limp 1.
infixr cimp 4.

type nao_atomico       form -> o.
type atomico           form -> o.
type expand       form -> form -> o.
```

Figura 13: Assinatura conectivos

```
module listas.

id nil nil.
id (X::L) (X::K) :- id L K.

membro X (X::L).
membro X (Y::L) :- membro X L.

append nil K K.
append (X::L) K (X::M) :- append L K M.

memb_and_rest X (X::L) L.
memb_and_rest X (Y::K) (Y::L) :- memb_and_rest X K L.

split nil nil nil.
split (X::L) (X::K) M :- split L K M.
split (X::L) K (X::M) :- split L K M.
```

Figura 14: Modulo listas

```
sig listas.

type id                list A -> list A -> o.
type membro            A -> list A -> o.
type append            list A -> list A -> list A -> o.
type memb_and_rest     A -> list A -> list A -> o.
type split        list A -> list A -> list A -> o.
```

Figura 15: Assinatura listas

Referências

[1] Andreoli, JM., *Logic programming with focusing proofs in linear logic*, Journal of Logic and Computation, vol. 2, no. 3, pp. 297–347 (1992).

[2] Appel, K., Haken, W. and Koch, J., *Every Planar map is Four Colorable*, Illinois: Journal of Mathematics, vol.21, pp. 439–567 (1977).

[3] Armstrong, E., et al, *The J2EE 1.4 Tutorial*, Sun Microsystems (2005).

[4] Barendregt, H.P., *The Lambda Calculus: its syntax and semantics*, N.103 in Studies in Logic and the Foundations of Mathematics (revised edition), North-Holland, Amsterdam (1994).

[5] Church, A., *A formulation of the simple theory of types*, Journal of Symbolic Logic 5, pp. 56–68 (1940).

[6] Dyckhoff, R. *Contraction-free sequent calculi for intuitionistic logic*, Journal of Symbolic Logic, vol. 7, pp. 795–807 (1992).

[7] A. Felty and D. Miller Specifying theorem provers in a higher-order logic programming language, *Ninth International Conference on Automated Deduction*, 1988.

[8] Gentzen, G., *Investigations into logical deductions*, The Collected Papers of Gerhard Gentzen, North-Holland Publishing Co., Amsterdam (1969).

[9] Girard, J-Y., *Linear Logic*, Theoretical Computer Science, vol 50, pp. 1–102 (1987).

[10] Girard, J-Y., *Proofs and types.*

[11] Gödel, K. *On Undecidable Propositions of Formal Mathematical Systems*, New York (1934).

[12] Hatcher, W. S. *Foundations of Mathematics* (1968).

[13] van Heijenoort, J., *From Frege to Gödel*, Harvard College, (1999).

[14] Hilbert, D., Ackermann, W., *Grundzüge der Theoretischen Logik*, Berlin, Springer (1928).

[15] Miller, D., Nadathur, G., Pfenning, F., and Scedrov, A., *Uniform proofs as a foundation for logic programming*, Annals of Pure and Applied Logic, vol.51 (1991).

[16] Miller, D., *Forum: A multiple-conclusion specification language*, Theoretical Computer Science, vol.165, pp. 201–232 (1996).

[17] Miller, D. *Sequent Calculus and the Specification of Computation*, School Marktoberdorf on Logic of Computation in 1997: An Advanced Study Institute of the NATO Science Committee and the Technical University of Munich, Germany (1997).

[18] Miller, D., Pimentel, E. *Using linear logic to reason about sequent systems*, Lecture Notes in Computer Science, v. 2381, pp. 2–23 (2002).

[19] Miller, D., Pimentel, E. *Linear logic as a framework for specifying sequent calculus*, Lecture Notes in Logic 17, pp. 111–135 (2004).

[20] G. Nadathur and D. Miller. An Overview of λ-Prolog. In *Fifth International Logic Programming Conference*, pp. 810–827, August 1988. MIT Press.

[21] Nadathur, G., *Teyjus: Language Manual*, http://teyjus.cs.umn.edu/language/teyjus_toc.html.

[22] Objective Calm, http://caml.inria.fr/ocaml/.

[23] Negri, S. and von Plato, J., *Structural proof theory*, Cambridge University Press (2001).

[24] Pimentel, E., Miller, D., *On the specification of sequent systems*, Lecture Notes in Computer Science, v. 3835, pp. 352 – 366 (2005).

[25] Pimentel, E., *Fundamentos de Matemática*, disponível em http://www.mat.ufmg.br/˜elaine/fundmat.pdf (2006).

[26] Pimentel, E., *PLLIC - fundamentação teórica*, disponível em http://www.mat.ufmg.br/˜elaine/PLLIC_teoria.pdf (2007).

[27] Prawitz, D., *Natural Deduction: a proof-theoretical study*, Dover Publications (2006).

[28] PVS Specification and Verification System, http://pvs.csl.sri.com.

[29] Ronchi Della Rocca S., Paolini L., *The Parametric λ-calculus: a metamodel for computation*, Computer Science-Monograph, Springer Verlag (2004).

[30] Russell, B. and Whitehead, A. N., *Principia Mathematica*, New York, Cambridge University Press (1927).

[31] Smullyan, R. M., *Gödel's incompletness theorems*, New York, Oxford University Press (1992).

[32] Smullyan, R. M., *Alice no país dos enigmas*, Rio de Janeiro, Jorge Zahar Editor (2000).

[33] Troelstra, A. S., *Lectures on Linear Logic*, CSLI (1992).

[34] Troelstra, A. S. and Schiwichtenberg, *Basic Proof Theory*, Cambridge University Press (2000).

[35] Van Dalen, Dirk, *Logic and Structure*, Springer Verlag (1991).