# ***Lógica e Estrutura***

(Versão Parcial: 14/12/2001, 10:55hs)

$\boxed{\text{Favor não distribuir}}$

Dirk van Dalen

Traduzido do original em inglês
***Logic and Structure,*** Springer, ©1980, 1983, 1994
(Segunda Edição Corrigida 1997)
por Ruy J. Guerra B. de Queiroz

# Prefácio

Lógica aparece sob forma 'sagrada' e sob forma 'profana'; a forma sagrada é predominante em teoria da prova, a forma profana em teoria dos modelos. O fenômeno não é incomum, observa-se essa dicotomia também em outras áreas, e.g. teoria dos conjuntos e teoria da recursão. Algumas catástrofes antigas, tais como a descoberta dos paradoxos da teoria dos conjuntos (Cantor, Russell), ou os paradoxos da definibilidade (Richard, Berry), nos fazem tratar um assunto por algum tempo com espanto e timidez. Mais cedo ou mais tarde, entretanto, as pessoas começam a tratar o assunto de uma maneira mais livre e mais fácil. Tendo sido educado na tradição 'sagrada', meu primeiro contato com a tradição profana foi algo como um choque cultural. Hartley Rogers me introduziu a um mundo mais descontraído da lógica através de seu exemplo de ensinar teoria da recursão a matemáticos como se fosse apenas um curso comum em, digamos, álgebra linear ou topologia algébrica. No decorrer do tempo acabei aceitando esse ponto de vista como o didaticamente seguro: antes de entrar para as belezas esotéricas seria preciso desenvolver um certo sentimento pelo assunto e obter uma quantidade razoável de conhecimento pleno de trabalho. Por essa razão este texto introdutório inicia-se na vertente profana e tende à sagrada apenas no final.

O presente livro foi desenvolvido a partir de cursos dados nos departamentos de matemática da Universidade de Utrecht. A experiência adquirida nesses cursos e a reação dos participantes sugeriram fortemente que não se deveria praticar e ensinar lógica em isolamento. Assim que possível exemplos cotidianos de matemática deveriam ser introduzidos; de fato, lógica de primeira ordem encontra um campo cheio de aplicações no estudo dos grupos, anéis, conjuntos parcialmente ordenados, etc.

O papel da lógica em matemática e ciência da computação tem dois aspectos — uma ferramenta para aplicações em ambas as áreas, e uma técnica para assentar os fundamentos. Esse último papel será neglicenciado aqui, e nos concentraremos nos problemas cotidianos da ciência formalizada (ou formalizável). De fato, optei por uma abordagem prática, — cobrirei o básico de técnicas de prova e de semântica, e passarei então para os tópicos que são menos abstratos. A experiência tem nos ensinado que a técnica de dedução natural de Gentzen se presta melhor para uma introdução, é próxima o suficiente do verdadeiro raciocínio informal para permitir que os estudantes construam as provas por si próprios. Praticamente nenhum truque artificial está envolvido e no final existe a agradável descoberta de que o sistema tem propriedades impressionantes, em particular ele se adequa perfeitamente à interpretação construtiva da lógica e permite formas normais. Esse último tópico foi adicionado a esta edição em vista de sua importância em teoria da computação. No capítulo 3 já temos poder técnico suficiente para obter alguns dos tradicionais e (mesmo hoje) surpreendentes resultados da teoria dos modelos.

O livro está escrito para principiantes sem conhecimento de tópicos mais avançados, nada de teoria esotérica dos conjuntos ou teoria da recursão. Os ingredientes básicos são dedução natural e semântica, esse último sendo apresentado tanto na forma construtiva quanto na forma clássica.

No capítulo 5 a lógica intuicionística é tratada com base na dedução natural sem a regra de Reductio ad absurdum, e da semântica de Kripke. A lógica intuicionística tem se livrado gradualmente da imagem de excentricidade e hoje é reconhecida por sua utilidade em e.g., teoria de topos e teoria de tipos, por isso sua inclusão em um texto introdutório é plenamente justificado. O capítulo final, sobre normalização, foi adicionado pelas mesmas razões; normalização tem um papel importante em certas partes da ciência da computação; tradicionalmente normalização (e eliminação do corte) pertence à teoria da prova, mas gradualmente aplicações em outras áreas têm sido introduzidas. No capítulo 6 consideramos apenas normalização fraca, e um número de aplicações simples é fornecido.

Várias pessoas têm contribuído para o perfil do texto em uma ocasião ou outra; Dana Scott, Jane Bridge, Henk Barendregt e Jeff Zucker foram muito importantes na preparação da primeira edição. Desde então muitos colegas e estudantes têm localizado erros e sugerido melhoramentos; esta edição teve o benefício de contar com as observações de Eleanor McDonnell, A. Scedrov e Karst Koymans. A todos esses críticos e consultores sou grato.

O progresso impôs que a máquina de datilografar tradicional deveria ser substituída por dispositivos mais modernos; este livro foi refeito em LaTeX por Addie Dekker e minha mulher Doke. Addie abriu caminho com as primeiras três seções do capítulo um e Doke concluiu o restante do manuscrito; devo a ambas, especialmente a Doke que encontrou tempo e coragem para dominar os secredos do LaTeX. Agradecimentos também a Leen Kievit por ter confeccionado as derivações e por ter adicionado o toque final necessário a um manuscrito LaTeX. A macro de Paul Taylor para árvores de prova foi usada para as derivações em dedução natural.

Junho 1994

A conversão para TEX introduziu um punhado de erros de impressão que estão corrigidos nesta nova tiragem. Muitos leitores têm sido bondosos me enviando sua coleção de erros de impressão, sou-lhes grato por sua ajuda. Em particular quero agradecer a Jan Smith, Vincenzo Scianna, A. Ursini, Mohammad Ardeshir e Norihiro Kamide. Aqui em Utrecht minhas turmas de lógica têm contribuído bastante, e em particular Marko Hollenberg, que ensinou parte de um curso, me passou comentários úteis. Gostaria de agradecê-los também.

Usei a ocasião para incorporar uns poucos melhoramentos. Algumas formulações foram modificadas de modo a torná-las mais precisas, e a definição de 'subfórmula' foi padronizada – juntamente com a noção de ocorrência positiva e negativa. Existe também um pequeno adendo sobre 'indução sobre a complexidade de uma fórmula'. Os exercícios 14 e 18 da seção 3.2 foram transferidos para a seção seguinte, pois eles são basicamente aplicações do lema do Diagrama.

Março 1997 Dirk van Dalen

# Índice

# Capítulo 0

# Introdução

Sem adotar uma das várias visões defendidas nos fundamentos da matemática, podemos concordar que matemáticos precisam e fazem uso de uma linguagem, mesmo se apenas para a comunicação de seus resultados e seus problemas. Enquanto matemáticos têm afirmado pela máxima possível exatidão para seus métodos, eles têm sido menos sensíveis com respeito a seu meio de comunicação. É bem conhecido que Leibniz propôs colocar a prática da comunicação matemática e do raciocínio matemático sobre uma base firme; entretanto, não foi antes do século dezenove que tais empreitadas foram levadas a cabo com mais sucesso por G. Frege e G. Peano. Independentemente do quão engenhosa e rigorosamente Frege, Russell, Hilbert, Bernays e outros desenvolveram a lógica matemática, foi apenas na segunda metade desse século que lógica e sua linguagem mostraram algumas características de interesse para o matemático em geral. Os resultados sofisticados de Gödel obviamente foram logo apreciados, mas eles permaneceram por um longo tempo como destaques técnicos mas sem uso prático. Até mesmo o resultado de Tarski sobr a decidibilidade da álgebra elementar e geometria tiveram que esperar seu momento adequado até que algumas aplicações aparecessem.

Hoje em dia as aplicações de lógica a álgebra, análise, topologia, etc. são em grande número e bem reconhecidas. Parece estranho que um bom número de fatos simples, dentro da capacidade de percepção de qualquer estudante, passassem despercebidos por tanto tempo. Não é possível dar o crédito apropriado a todos aqueles que abriram esse novo território, qualquer lista demonstraria inevitavelmente as preferências do autor, e omitiria algumas áreas e pessoas.

Vamos observar que matemática tem uma maneira bem regular, canônica de formular seu material, em parte por sua natureza sob a influência de fortes escolas, como a de Bourbaki. Além do mais, a crise no início do século forçou os matemáticos a prestar mais atenção aos detalhes mais finos de sua linguagem e às suas pressuposições concernentes à natureza e o alcance do universo matemático. Essa atenção começou a dar frutos quando se descobriu que havia em certos casos uma estreita ligação entre classes de estruturas matemáticas e suas descrições sintáticas. Aqui vai um exemplo:

Sabe-se bem que um subconjunto de um grupo $G$ que é fechado sob multiplicação e inverso, é um grupo; entretanto, um subconjunto de um corpo algebricamente fechado $F$ que é fechado sob soma, produto, menos e inverso, é em geral um corpo que não é algebricamente fechado. Esse fenômeno é uma instância de algo bem geral: uma classe axiomatizável de estruturas é axiomatizada por um conjunto de sentenças universais (da forma $\forall x_1, \ldots, x_n \varphi$, com $\varphi$ sem-quantificadores) sse ela é fechada sob subestruturas. Se verificarmos os axiomas da teoria dos grupos veremos que de fato todos os axiomas são universais, enquanto que nem todos os axiomas da teoria dos corpos algebricamente fechados são universais. Esse último fato poderia obviamente ser acidental, poderia ser o caso que não fôssemos espertos o suficiente para descobrir uma axiomatização universal da classe de corpos algebricamente fechados. O teorema acima de Tarski e Los nos diz, entretanto, que é impossível encontrar tal axiomatização!

O ponto de interesse é que para algumas propriedades de uma classe de estruturas temos critérios sintáticos simples. Podemos, por assim dizer, ler o comportamento do mundo matemático real (em alguns casos simples) a partir de sua descrição sintática.

Existem numerosos exemplos do mesmo tipo, e.g. o *Teorema de Lyndon*: uma classe axiomatizável de estruturas é fechada sob homomorfismos sse ela pode ser axiomatizada por um conjunto de sentenças positivas (i.e. sentenças que, em forma normal prenex com a parte aberta em forma normal disjuntiva, não contêm negação).

O exemplo mais básico e ao mesmo tempo monumental de tal ligação entre noções sintáticas e o universo matemático é obviamente o *teorema da completude de Gödel*, que nos diz que demonstrabilidade nos sistemas formais usuais é extensionalmente idêntica à noção de *verdade* em todas as estruturas. Isto é o mesmo que dizer, embora demonstrabilidade e verdade sejam noções totalmente diferentes (a primeira é combinatorial por natureza, e a outra é conjuntista), elas determinam a mesma classe de sentenças: $\varphi$ é demonstrável sse $\varphi$ é verdadeira em todas as estruturas.

Dado que o estudo de lógica envolve uma boa dose de trabalho sintático, iniciaremos apresentando uma maquinaria eficiente para lidar com sintaxe. Usamos a técnica de *definições indutivas* e como uma conseqüência ficamos bem inclinados a ver árvores onde for possível, em particular preferimos dedução natural na forma de árvores às versões lineares que aparecem aqui e ali em uso na literatura.

Um dos fenômenos impressionantes no desenvolvimento dos fundamentos da matemática é a descoberta de que a própria linguagem da matemática pode ser estudada por meios matemáticos. Isso está longe de ser um jogo fútil: os teoremas da incompletude de Gödel, por exemplo, e o trabalho de Gödel e Cohen no campo das provas de independência em teoria dos conjuntos requerem um minucioso conhecimento da matemática e da linguagem matemática. Esses tópicos não fazem parte do escopo do presente livro, portanto podemos nos concentrar nas partes mais simples da sintaxe. Entretanto objetivaremos fazer um tratamento minucioso, na esperança de que o leitor perceberá que todas essas coisas que ele suspeita ser trivial, mas não consegue ver por que, são perfeitamente acessíveis a demonstrações. Ao leitor pode ser uma ajuda pensar de si próprio como um computador com enormes capacidades mecânicas, mas sem qualquer estalo criativo, naqueles casos em que fica intrigado devido a questões do tipo 'por que devemos provar algo tão completamente evidente'!

Por outro lado o leitor deve sempre se lembrar que ele não é um computador e que, certamente quando ele chegar ao capítulo 3, alguns detalhes devem ser reconhecidos como triviais.

Para a prática propriamente dita da matemática a lógica de predicados é sem dúvida a ferramenta perfeita, pois ela nos permite manusear objetos individualmente. Mesmo assim iniciamos o livro com uma exposição da lógica proposicional. Há várias razões para essa escolha.

Em primeiro lugar a lógica proposicional oferece em miniatura os problemas que encontramos na lógica de predicados, mas lá as dificuldades obscurecem alguns dos aspectos relevantes e.g. o teorema da completude para a lógica proposicional já usa o conceito de 'conjunto consistente maximal', mas sem as complicações dos axiomas de Henkin.

Em segundo lugar existem um número de questões verdadeiramente proposicionais que seriam difíceis de tratar em um capítulo sobre a lógica de predicados sem criar uma impressão de descontinuidade que se aproxima do caos. Finalmente parece uma questão de pedagogia saudável deixar que a lógica proposicional preceda a lógica de predicados. O principiante pode em um único contexto se familiarizar com as técnicas de teoria da prova, as algébricas e as da teoria dos modelos que seria demasiado em um primeiro contato com a lógica de predicados.

Tudo o que foi dito sobre o papel da lógica em matemática pode ser repetido para a ciência da computação; a importância dos aspectos sintáticos é ainda mais pronunciada que em matemática, mas não pára aqui. A literatura de teoria da computação é abundante em sistemas lógicos, provas de completude e coisas do gênero. No contexto de teoria dos tipos (lambda cálculo tipificado) a lógica intuicionística tem adquirido um papel importante, enquanto que as técnicas de normalização têm se tornado uma dieta básica para cientistas da computação.

# Capítulo 1

# Lógica Proposicional

## 1.1 Proposições e Conectivos

Tradicionalmente, lógica é dita ser a arte (ou estudo) do raciocínio; portanto para descrever a lógica na sua tradição, temos que saber o que é 'raciocínio'. De acordo com algunas visões tradicionais o raciocínio consiste do processo de construir cadeias de entidades lingüísticas por meio de certas relações '... segue de ...', uma visão que é suficientemente boa para nossos propósitos. As entidades lingüísticas que ocorrem nesse tipo de raciocínio são tomadas como sendo *sentenças*, i.e. entidades que exprimem um pensamento completo, ou estado de coisas. Chamamos tais sentenças de *declarativas*. Isso significa que, do ponto de vista da língua natural nossa classe de objetos lingüísticos aceitáveis é bastante restrita.

Felizmente essa classe é suficientemente larga quando olhada do ponto de vista do matemático. Até o presente a lógica tem sido capaz de caminhar muito bem mesmo com essa restrição. É verdade, não se pode lidar com perguntas, ou enunciados imperativos, mas o papel desses entidades é desprezível em matemática pura. Devo fazer uma exceção a enunciados de ação, que têm um papel importante em programação; pense em instruções como 'goto, if ... then, else ...', etc. Por razões dadas adiante, vamos, no entanto, deixá-las de fora.

As sentenças que temos em mente são do tipo '27 é um número quadrado', 'todo inteiro positivo é a soma de quatro quadrados', 'existe apenas um conjunto vazio'. Um aspecto comum de todas essas sentenças declarativas é a possibilidade de atribuí-las um valor de verdade, *verdadeiro* ou *falso*. Não exigimos a determinação propriamente dita do valor de verdade em casos concretos, como por exemplo a conjectura de Goldbach ou a hipótese de Riemann. Basta que possamos 'em princípio' atribuir um valor de verdade.

Nossa chamada lógica *bi-valorada* é baseada na suposição de que toda sentença é verdadeira ou falsa, e é a pedra angular da prática de tabelas-verdade.

Algumas sentenças são mínimas no sentido de que não há parte própria que seja também uma sentença, e.g. $5 \in \{0, 1, 2, 5, 7\}$, ou $2+2 = 5$; outras podem ser divididas em partes menores, e.g. '$c$ é um racional ou $c$ é um irracional' (onde $c$ é uma constante). Por outro lado, podemos construir sentenças maiores a partir de sentenças menores através do uso de *conectivos*. Conhecemos muitos conectivos em língua natural; a seguinte lista não tem de forma alguma o propósito de ser exaustiva: *e*, *ou*, *não*, *se* ... *então* ..., *mas*, *pois*, *como*, *por*, *embora*, *nem*. No discurso usual, como também em matemática informal, usa-se esses conectivos incessantemente; entretanto, em matemática formal seremos econômicos nos conectivos que admitimos. Isso é sobretudo por razões de exatidão. Compare, por exemplo, as seguintes sentenças: "$\pi$ é irracional, mas não é algébrico", "Max é um marxista, mas ele não é carrancudo". No segundo enunciado podemos descobrir uma sugestão de algum contraste, como se deveríamos nos surpreender que Max não é carrancudo. No primeiro caso tal surpresa não pode ser facilmente imaginada (a menos que, e.g. se tenha acabado de ler que todos os irracionais são algébricos); sem modificar o significado pode-se transformar esse enunciado em "$\pi$ é irracional e $\pi$ não é algébrico". Logo por que usar (em um texto formal) a formulação que traz certos tons vagos, emocionais? Por essas e outras razões (e.g. de economia) em lógica nos fixamos em um número limitado de conectivos, em particular aqueles que têm-se mostrado úteis na rotina diária de formular e demonstrar.

Note, entretanto, que mesmo aqui as ambigüidades ameaçam. Cada um dos conectivos já tem um ou mais significados em língua natural. Vamos dar alguns exemplos:

1. João passou direto e bateu num pedestre.
2. João bateu num pedestre e passou direto.
3. Se eu abrir a janela então termos ar fresco.
4. Se eu abrir a janela então $1 + 3 = 4$.
5. Se $1 + 2 = 4$, então teremos ar fresco.
6. João está trabalhando ou está em casa.
7. Euclides foi um grego ou um matemático.

De 1 e 2 concluimos que 'e' pode ter uma função de ordenação no tempo. Não é assim em matemática; "$\pi$ é irracional e 5 é positivo" simplesmente significa que ambas as partes se verificam. O tempo simplesmente não tem qualquer papel na matemática formal. Certamente não poderíamos dizer "$\pi$ não era nem algébrico nem transcendente antes de 1882". O que desejaríamos dizer é que "antes de 1882 não se sabia se $\pi$ era algébrico ou transcendente".

Nos exemplos 3–5 consideramos a implicação. O exemplo 3 será em geral aceito, pois mostra um aspecto que viemos a aceitar como inerente à implicação: existe uma relação entre a premissa e a conclusão. Esse aspecto está ausente nos exemplos 4 e 5. Mesmo assim permitiremos casos tais como o 4 e o 5 em matemática. Há várias razões para se fazer isso. Uma é que a consideração de que o significado deveria ser deixado fora de considerações sintáticas. Do contrário a sintaxe se tornaria difícil de manejar e acabaríamos sendo levados a uma prática esotérica de casos excepcionais. Essa implicação generalizada, em uso em matemática, é chamada de *implicação material*. Algumas outras implicações têm sido estudadas sob as denominações de *implicação estrita*, *implicação relevante*, etc.

Finalmente 6 e 7 demonstram o uso do 'ou'. Tendemos a aceitar 6 e a rejeitar 7. Na maioria das vezes se pensa no 'ou' como algo exclusivo. Em 6 até certo ponto esperamos que João não trabalhe em casa, enquanto que 7 é incomum no sentido de que via de regra não usamos 'ou' quando poderíamos de fato usar 'e'. Além disso, normalmente hesitamos em usar uma disjunção se já sabemos qual das duas partes se verifica, e.g. "32 é um número primo ou 32 não é um número primo" será considerada (no mínimo) artificial pela maioria das pessoas, pois já sabemos que 32 não é um número primo. Ainda assim a matemática usa livremente tais disjunções supérfluas, por exemplo "$2 \geq 2$" (que designa "$2 > 2$ ou $2 = 2$").

De forma a prover a matemática de uma linguagem precisa criaremos uma linguagem artificial, formal, que se prestará ao tratamento matemático. Primeiramente definiremos uma linguagem para a lógica proposicional, i.e. a lógica que lida com *proposições* (sentenças, enunciados). Mais adiante estenderemos nosso tratamento à lógica que também leva em conta propriedades de objetos.

O processo de *formalização* da lógica proposicional consiste de dois estágios: (1) apresentar uma linguagem formal, (2) especificar um procedimento para se obter proposições *válidas* ou *verdadeiras*.

Inicialmente descreveremos a linguagem, usando a técnica de *definições indutivas*. O procedimento é bem simples: *Primeiro* especifique quem são as proposições menores, que não decomponíveis em proposições menores que elas; *depois* descreva como proposições compostas são construídas a partir de proposições previamente dadas.

**Definição 1.1.1** A linguagem da lógica propositional tem um alfabeto consistindo de
(i) *símbolos proposicionais*: $p_0, p_1, p_2, \ldots$,
(ii) *conectivos*: $\wedge$, $\vee$, $\rightarrow$, $\neg$, $\leftrightarrow$, $\perp$,
(iii) *símbolos auxiliares*: ( , ).

Os conectivos carregam nomes tradicionais:

| | | | | |
|---|---|---|---|---|
| $\wedge$ | - | *e* | - | *conjunção* |
| $\vee$ | - | *ou* | - | *disjunção* |
| $\rightarrow$ | - | *se ..., então ...* | - | *implicação* |
| $\neg$ | - | *não* | - | *negação* |
| $\leftrightarrow$ | - | *sse* | - | *equivalência, bi-implicação* |
| $\perp$ | - | *falso* | - | *falsum, absurdum* |

Os símbolos proposicionais e o símbolo $\perp$ designam proposições indecomponíveis, que chamamos *átomos*, ou *proposições atômicas*.

**Definição 1.1.2** O conjunto $PROP$ de proposições é o menor conjunto $X$ com as propriedades
$(i)$ $p_i \in X$ $(i \in N)$, $\perp \in X$,
$(ii)$ $\varphi, \psi \in X \Rightarrow (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \rightarrow \psi), (\varphi \leftrightarrow \psi) \in X$,
$(iii)$ $\varphi \in X \Rightarrow (\neg\varphi) \in X$.

As cláusulas descrevem exatamente as maneiras possíveis de construir proposições. De modo a simplificar a cláusula $(ii)$ escrevemos $\varphi, \psi \in X \Rightarrow (\varphi \Box \psi) \in X$, onde $\Box$ é um dos conectivos $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.

Uma advertência ao leitor é recomendável nesse ponto. Usamos letras gregas $\varphi, \psi$ na definição; elas são proposições? Claramente não queremos que elas sejam, pois queremos apenas aquelas cadeias de símbolos obtidas combinando-se símbolos do alfabeto de maneira correta. Evidentemente nenhuma letra grega entra de jeito nenhum! A explicação é que $\varphi$ e $\psi$ são usadas como variáveis para proposições. Como queremos estudar lógica, devemos usar uma linguagem para discutí-la nessa linguagem. Em geral essa linguagem é o português puro, cotidiano. Chamamos a linguagem usada para discutir lógica de nossa *meta-linguagem* e $\varphi$ e $\psi$ são *meta-variáveis* para proposições. Poderíamos dispensar meta-variáveis lidando com (ii) e (iii) verbalmente: se duas proposições são dadas, então uma nova proposição é obtida colocando-se o conectivo $\wedge$ entre elas e adicionando-se parênteses na frente e no final, etc. Essa versão verbal deveria bastar para convencer o leitor das vantagens da maquinaria matemática.

Note que adicionamos um conectivo um bocado incomum, $\perp$. Incomum no sentido de que ele não conecta nada. *Constante lógica* seria um nome melhor. Por uniformidade ficamos com o nosso uso já mencionado. $\perp$ é adicionado por conveniência, poder-se-ia muito bem dispensá-lo, mas ele tem certas vantagens. Pode-se notar que há algo faltando, nomeadamente um símbolo para a proposição verdadeira; de fato adicionaremos um outro símbolo, $\top$, como uma abreviação para a proposição "verdadeira".

*Exemplos.*

$$(p_7 \to p_0), ((\perp \vee p_{32}) \wedge (\neg p_2)) \in PROP.$$
$$p_1 \leftrightarrow p_7, \neg\neg\perp, ((\to \wedge \notin PROP$$

É fácil mostrar que algo pertence a $PROP$ (simplesmente execute a construção de acordo com 1.1.2); é um pouco mais difícil mostrar que algo não pertence a $PROP$. Faremos um exemplo:

$$\neg\neg\perp \notin PROP.$$

Suponha que $\neg\neg\perp \in X$ e $X$ satisfaz (i), (ii), (iii) da definição 1.1.2. Alegamos que $Y = X - \{\neg\neg\perp\}$ também satisfaz (i), (ii) e (iii). Como $\perp, p_i \in X$, também $\perp, p_i \in Y$. Se $\varphi, \psi \in Y$, então $\varphi, psi \in X$. Como $X$ satisfaz (ii) $(\varphi\Box\psi) \in X$. Da forma das expressões fica claro que $(\varphi\Box\psi) \neq \neg\neg\perp$ (olhe para os parênteses), logo $(\varphi\Box\psi) \in X - \{\neg\neg\perp\} = Y$. Igualmente se demonstra que $Y$ satisfaz (iii). Logo $X$ não é o menor conjunto satisfazendo (i), (ii) e (iii), portanto $\neg\neg\perp$ não pode pertencer a $PROP$.

Propriedades de proposições são estabelecidas por um procedimento indutivo análogo à definição 1.1.2: primeiro lida com os átomos, e depois vai das partes às proposições compostas. Isso é expresso mais precisamente em

**Teorema 1.1.3 (Princípio da indução)** *Seja $A$ uma propriedade, então $A(\varphi)$ se verifica para todo $\varphi \in PROP$ se*

(*i*) $A(p_i)$, *para todo* $i$, *e* $A(\perp)$,
(*ii*) $A(\varphi)$, $A(\psi) \Rightarrow A((\varphi\Box\psi))$,
(*iii*) $A(\varphi) \Rightarrow A((\neg\varphi))$.

*Demonstração.* Seja $X = \{\varphi \in PROP \mid A(\varphi)\}$, então $X$ satisfaz (i), (ii) e (iii) da definição 1.1.2. Logo $PROP \subseteq X$, i.e. para todo $\varphi \in PROP$ $A(\varphi)$ se verifica. $\Box$

A uma aplicação do teorema 1.1.3 chamamos de uma *prova por indução sobre* $\varphi$. O leitor vai notar uma semelhança óbvia entre o teorema acima e o princípio da indução completa em aritmética.

O procedimento acima que permite obter todas as proposições e provar propriedades de proposições é elegante e perspicaz; existe uma outra abordagem, no entanto, que tem suas próprias vantagens (em particular para codificação): considere proposições como o resultado de uma construção linear passo-a-passo. E.g. $((\neg p_0) \to \bot)$ é construído montando-se a expressão a partir de suas partes menores usando as partes previamente construídas: $p_0 \ldots \bot\ (\neg p_0) \ldots ((\neg p_0) \to \bot)$. Isso é formalizado da seguinte maneira:

**Definição 1.1.4** Uma seqüência $\varphi_0, \ldots, \varphi_n$ é chamada de *seqüência de formação* de $\varphi$ se $\varphi_n = \varphi$ e para todo $i \leq n$ $\varphi_i$ é atômica, ou

$$\begin{aligned} &\varphi_i = (\varphi_j \Box \varphi_k) \text{ para certo } j, k < i \text{ ou} \\ &\varphi_i = (\neg \varphi_i) \text{ para certo } j < i. \end{aligned}$$

Observe que nessa definição estamos considerando cadeias $\varphi$ de símbolos do alfabeto dado; isso abusa um pouco da convenção notacional.

*Exemplos.* (a) $\bot, p_2, p_3, (\bot \vee p_2), (\neg(\bot \vee p_2)), (\neg p_3)$ e $p_3, (\neg p_3)$ são ambas seqüências de formação de $(\neg p_3)$. Note que seqüências de formação podem conter 'lixo'.

(b) $p_2$ é uma subfórmula de $((p_7 \vee (\neg p_2)) \to p_1)$; $(p_1 \to \bot)$ é uma subfórmula de $(((p_2 \vee (p_1 \wedge p_0)) \leftrightarrow (p_1 \to \bot))$.

Agora vamos dar alguns exemplos triviais de prova por indução. Na prática apenas verificamos verdadeiramente as cláusulas da prova por indução e deixamos a conclusão para o leitor.

1. *Cada proposição tem um número par de parênteses.*

*Demonstração.* (i) Cada átomo tem 0 parênteses e 0 é par.

(ii) Suponha que $\varphi$ e $\psi$ tenham $2n$, resp. $2m$ parênteses, então $(\varphi \Box \psi)$ tem $2(n + m + 1)$ parênteses.

(iii) Suponha que $\varphi$ tem $2n$ parênteses, então $(\neg\varphi)$ tem $2(n + 1)$ parênteses. □

2. *Cada proposição tem uma seqüência de formação.*

*Demonstração.* (i) Se $\varphi$ é um átomo, então a seqüência consistindo de apenas $\varphi$ é uma seqüência de formação de $\varphi$.

(ii) Sejam $\varphi_0, \ldots, \varphi_n$ e $\psi_0, \ldots, \psi_m$ seqüências de formação de $\varphi$ e $\psi$, então observa-se facilmente que $\varphi_0, \ldots, \varphi_n, \psi_0, \ldots, \psi_m, (\varphi_n \Box \psi_m)$ é uma seqüência de formação de $(\varphi_n \Box \psi_m)$.

(iii) Deixo para o leitor. □

Podemos melhorar 2:

**Teorema 1.1.5** *PROP é o conjunto de todas as expressões que têm seqüência de formação.*

*Demonstração.* Seja $F$ o conjunto de todas as expressões (i.e. cadeias de símbolos) que têm seqüência de formação. Demonstramos acima que $PROP \subseteq F$.

Suponha que $\varphi$ tem uma seqüência de formação $\varphi_0, \ldots, \varphi_n$, vamos demonstrar que $\varphi \in PROP$ por indução sobre $n$.

$n = 0 : \varphi = \varphi_0$ e por definição $\varphi$ é atômica, logo $\varphi \in PROP$.

Suponha que todas as expressões com seqüência de formação de comprimento $m < n$ estão em $PROP$. Por definição $\varphi_n = (\varphi_i \Box \psi_j)$ para todo $i, j < n$, ou $\varphi_n = (\neg\varphi_i)$ para $i < n$, ou $\varphi_n$ é atômica. No primeiro caso $\varphi_i$ e $\varphi_j$ têm seqüência de formação de comprimento $i, j < n$, logo pela hipótese da indução $\varphi_i, \varphi_j \in PROP$. Como $PROP$ satisfaz às cláusulas de definição 1.1.2, temos também $(\varphi_i \Box \varphi_j) \in PROP$. Trate negação igualmente. O caso atômico é trivial. Conclusão $F \subseteq PROP$. □

Em um certo sentido o Teorema 1.1.5 é uma justificação da definição de seqüência de formação. Ele também nos permite estabelecer propriedades de proposições por indução ordinária sobre o comprimento de seqüências de formação.

Em aritmética normalmente se define funções por recursão, e.g. exponenciação é definida por $x^0 = 1$, e $x^{y+1} = x^y \cdot x$, ou a função fatorial por $0! = 1$ e $(x+1)! = x! \cdot (x+1)$. A justificação é bem imediata: cada valor é obtido usando-se os valores precedentes (para argumentos positivos). Existe um princípio análogo em nossa sintaxe.

*Exemplos.* O número $p(\varphi)$ de parênteses de $\varphi$, pode ser definido como se segue:

$$\begin{cases} p(\varphi) & = 0 \text{ para } \varphi \text{ atômica,} \\ p((\varphi \Box \psi)) & = p(\varphi) + p(\psi) + 2, \\ p((\neg\varphi)) & = p(\varphi) + 2. \end{cases}$$

O valor de $p(\varphi)$ pode ser computado calculando-se sucessivamente $p(\psi)$ para as subfórmulas $\psi$. □

Podemos dar esse tipo de definição para todos os conjuntos que são definidos por indução. O princípio de "definição por recursão" toma a forma de "existe uma única função tal que ...". O leitor deve se manter lembrado que a idéia básica é que pode-se 'computar' o valor da função para uma composição de uma forma prescrita a partir dos valores da função nas partes componentes.

O princípio geral por trás dessa prática é firmado pelo seguinte teorema.

**Teorema 1.1.6 (Definição por Recursão)** *Suponha que sejam dados os mapeamentos $H_\Box : A^2 \to A$ e $H_\neg : A \to A$ e suponha que $H_{at}$ seja um mapeamento do conjunto de átomos para $A$, então existe exatamente um mapeamento $F : PROP \to A$ tal que*

$$\begin{cases} F(\varphi) & = H_{at} \text{ para } \varphi \text{ atômica,} \\ F((\varphi \Box \psi)) & = H_\Box(F(\varphi), F(\psi)), \\ F((\neg\varphi)) & = H_\neg(F(\varphi)). \end{cases}$$

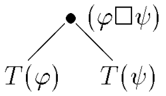
Usualmente, em aplicações concretas o princípio é bem facilmente reconhecido como um princípio correto. Entretanto, em geral tem-se que demonstrar a existência de uma única função satisfazendo às equações acima. A demonstração é deixada como um exercício, cf. Exercício 11.

Aqui estão algums exemplos de definição por recursão:

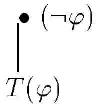
1. A *árvore* (léxica) de uma proposição $\varphi$ é definida por

$T(\varphi) \quad = \quad \bullet\ \varphi \quad$ para $\varphi$ atômica

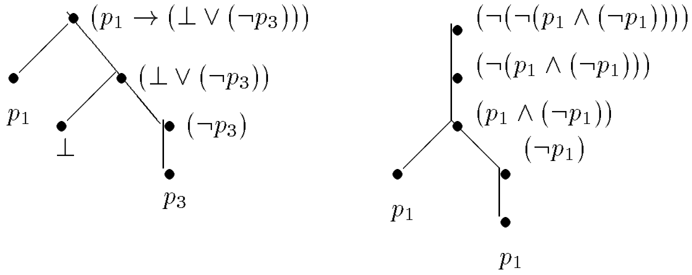
$T((\varphi\Box\psi)) =$




$T((\neg\varphi)) \quad =$

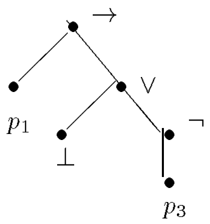



*Exemplos.* $\quad T((p_1 \to (\bot \vee (\neg p_3)))$; $\quad T(\neg(\neg(p_1 \wedge (\neg p_1))))$

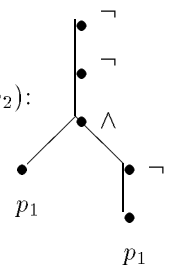



Uma maneira simples de exibir as árvores consiste em listar os átomos localizados no fundo, e indicar os conectivos presentes nos nós.

$T(\varphi_1)$:




$T(\varphi_2)$:




2. O *posto* $p(\varphi)$ de uma proposição $\varphi$ é definido por

$$\begin{cases} p(\varphi) & = 0 \text{ para } \varphi \text{ atômica,} \\ p((\varphi\Box\psi)) & = \max(p(\varphi), p(\psi)) + 1, \\ p((\neg\varphi)) & = p(\varphi) + 1. \end{cases}$$

Agora vamos usar a técnica da definição por recursão para definir a noção de subfórmula.

**Definição 1.1.7** O conjunto das subfórmulas $Sub(\varphi)$ é dado por

$$\begin{array}{ll} Sub(\varphi) & = \{\varphi\} \text{ para } \varphi \text{ atômica} \\ Sub(\varphi_1\Box\varphi_2) & = Sub(\varphi_1) \cup Sub(\varphi_2) \cup \{\varphi_1\Box\varphi_2\} \\ Sub(\neg\varphi) & = Sub(\varphi) \cup \{\neg\varphi\} \end{array}$$

Dizemos que $\psi$ *é uma subfórmula de* $\varphi$ se $\varphi \in Sub(\varphi)$.

*Convenções de notação.* De forma a simplificar nossa notação vamos economizar em parênteses. Vamos sempre desprezar os parênteses mais externos e omitiremos também os parênteses no caso de negações. Além do mais usaremos a convenção que $\wedge$ e $\vee$ têm precedência sobre $\rightarrow$ e $\leftrightarrow$ (cf. $\cdot$ e $+$ em aritmética), e que $\neg$ tem precedência sobre os outros conectivos.

*Exemplos.*

| | | |
|---|---|---|
| $\neg\varphi \vee \varphi$ | designa | $((\neg\varphi) \vee \varphi)$, |
| $\neg(\neg\neg\neg\varphi \wedge \bot)$ | designa | $(\neg((\neg(\neg(\neg\varphi))) \wedge \bot))$, |
| $\varphi \vee \psi \rightarrow \varphi$ | designa | $((\varphi \vee \psi) \rightarrow \varphi)$, |
| $\varphi \rightarrow \varphi \vee (\psi \rightarrow \chi)$ | designa | $(\varphi \rightarrow (\varphi \vee (\psi\chi)))$. |

*Advertência.* Note que, rigorosamente falando, aquelas abreviações não são proposições.

Na proposição $(p_1 \rightarrow p_1)$ apenas um átomo é usado para definí-la, embora ele seja usado duas vezes e ocorra em dois lugares. Para um certo propósito é conveniente distinguir entre *fórmulas* e *ocorrências de fórmulas*. A definição de subfórmula não nos informa o que é uma ocorrência de $\varphi$ em $\psi$, por isso temos que adicionar alguma informação. Uma maneira de indicar uma ocorrência de $\varphi$ é especificar seu lugar na árvore de $\psi$, e.g. uma ocorrência de uma fórmula em uma dada fórmula $\psi$ é um par $(\varphi, k)$, onde $k$ é um nó na árvore de $\psi$. Poder-se-ia até mesmo codificar $k$ como uma seqüência de 0's e 1's, onde associamos a cada nó a seguinte seqüência: $\langle\ \rangle$ (a seqüência vazia) para o nó raiz, $\langle s_0, \ldots, s_{n-1}, 0\rangle$ para o descendente imediato à esquerda do nó com seqüência $\langle s_0, \ldots, s_{n-1}\rangle$ e $\langle s_0, \ldots, s_{n-1}, 1\rangle$ para o seu segundo descendente imediato (se existe algum). Não seremos demasiadamente formais no manuseio de ocorrências de fórmulas (ou símbolos, na verdade), mas é importante que isso pode ser feito.

A introdução da função de posto não é mera ilustração da 'definição por recursão', pois ela também nos permite demonstrar fatos sobre proposições por meio da *indução completa* (ou *indução matemática*). Reduzimos, por assim dizer, a estrutura de árvore à linha reta dos números naturais. Note que outras 'medidas' servirão tão bem quanto essa, e.g. o número de símbolos. Para evitar omissão definiremos explicitamente o *Princípio da Indução sobre o Posto*:

**Teorema 1.1.8 (Princípio da indução sobre o posto)** *Se para todo $\varphi$ [$A(\psi)$ para todo $\psi$ com posto menor que $p(\varphi)$] $\Rightarrow A(\varphi)$, então $A(\varphi)$ se verifica para todo $\varphi \in PROP$.*

Vamos mostrar que indução sobre $\varphi$ e indução sobre o posto de $\varphi$ são equivalentes.[1]

Primeiro introduzimos uma notação conveniente pra a indução sobre o posto: escreva $\varphi \prec \psi$ ($\varphi \preceq \psi$) para designar $p(\varphi) < p(\psi)$ ($p(\varphi) \leq p(\psi)$). Logo $\forall\psi \preceq \varphi\, A(\varphi)$ designa "$A(\psi)$ se verifica para todo $\psi$ com posto no máximo $p(\varphi)$"

O *Princípio da Indução sobre o Posto* agora lê

$$\forall\varphi(\forall\psi \preceq \varphi\, A(\psi) \Rightarrow A(\varphi)) \Rightarrow \forall\varphi\, A(\varphi)$$

[1] O leitor pode pular essa demonstração na primeira leitura. Estará fazendo bem aplicando a indução sobre o posto ingenuamente.

Demonstraremos que o princípio da indução sobre o posto segue do princípio da indução. Suponha que

$$\forall\varphi(\forall\psi \preceq \varphi\, A(\psi) \Rightarrow A(\varphi)) \qquad (\dagger)$$

seja dado. Para mostrar que $\forall\varphi\, A(\varphi)$ temos que comer do próprio bolo, ou seja, usar um pouco de indução. Ponha $B(\varphi) := \forall\psi \preceq \varphi\, A(\varphi)$. Agora vamos demonstrar $\forall\varphi\, B(\varphi)$ por indução sobre $\varphi$.

1. para $\varphi$ atômica $\forall\psi \prec \varphi\, A(\varphi)$ é vacuamente verdadeira, logo por ($\dagger$) $A(\varphi)$ se verifica. Portanto $A(\psi)$ se verifica para todo $\psi$ com posto $\leq 0$. Logo $B(\varphi)$.

2. $\varphi = \varphi_1 \square \varphi_2$. Hipótese da indução: $B(\varphi_1)$, $B(\varphi_2)$. Seja $\rho$ uma proposição qualquer com $p(\rho) = p(\varphi) = n + 1$ (para um $n$ apropriado). Temos que demonstrar que $\rho$ e todas as proposições com posto menor que $n + 1$ têm a propriedade $A$. Como $p(\varphi) = max(p(\varphi_1), p(\varphi_2)) + 1$, ou $\varphi_1$ ou $\varphi_2$ tem posto $n$ — digamos $\varphi_1$. Agora escolha um $\psi$ arbitrário com $p(\psi) \leq n$, então $\psi \preceq \varphi_1$. Portanto, por $B(\varphi_1)$, $A(\psi)$ se verifica. Isso demonstra que $\forall\psi \prec \rho\, A(\psi)$, logo por ($\dagger$) $A(\rho)$ se verifica. Isso demonstra $B(\varphi)$.

3. $\varphi = \neg\varphi_1$. Argumento semelhante.

Uma aplicação do princípio da indução nos dá $\forall\varphi\, B(\varphi)$, e como uma conseqüência $\forall\varphi\, A(\varphi)$.

Para a recíproca assumimos as premissas do princípio da indução. Para aplicar o princípio da indução sobre o posto temos que mostrar que ($\dagger$) se verifica. Distinguimos os seguintes casos:

1. $\varphi$ atômica. Então ($\dagger$) trivialmente se verifica.

2. $\varphi = \varphi_1 \square \varphi_2$. Então $\varphi_1, \varphi_2 \preceq \varphi$ (veja exercício 6). Nossa hipótese é $\forall\psi \prec \varphi\, A(\psi)$, portanto $A(\varphi_1)$ e $A(\varphi_2)$ se verificam. Logo $A(\varphi)$ se verifica.

3. $\varphi = \neg\varphi_1$. Argumento semelhante.

Isso estabelece ($\dagger$). Logo pela indução sobre o posto obtemos $\forall\varphi\, A(\varphi)$.

### Exercícios

1. Dê as seqüências de formação de

   $(\neg p_2 \to (p_3 \vee (p_1 \leftrightarrow p_2))) \wedge \neg p_3$,

   $(p_7 \to \neg\bot) \leftrightarrow ((p_4 \wedge \neg p_2) \to p_1)$,

   $(((p_1 \to p_2) \to p_1) \to p_2) \to p_1$.

2. Demonstre que $((\to \notin PROP$.

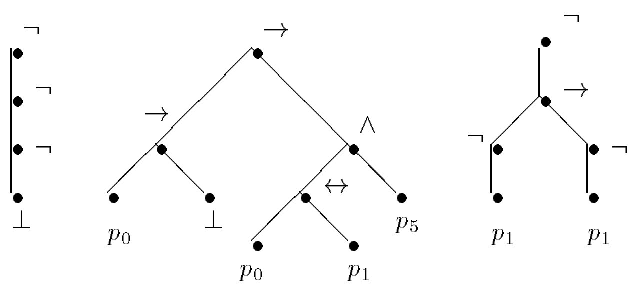
3. Demonstre que a relação "é uma subfórmula de" é transitiva.

4. Seja $\varphi$ uma subfórmula de $\psi$. Demonstre que $\varphi$ ocorre em cada seqüência de formação de $\psi$.

5. Se $\varphi$ ocorre em uma seqüência de formação mínima de $\psi$ então $\varphi$ é uma subfórmula de $\psi$.

6. Seja $g$ a função posto:
   (a) Demonstre que $p(\varphi) \leq$ o número de ocorrências de conectivos de $\varphi$,
   (b) Dê exemplos de $\varphi$ tais que $<$ ou $=$ se verifica em (a),
   (c) Ache o posto das proposições no exercício 1.
   (d) Demonstre que $p(\varphi) < p(\psi)$ se $\varphi$ é uma subfórmula própria de $\psi$.

7. (a) Determine as árvores das proposições no exercício 1,
   (b) Determine as proposições com as seguintes árvores.




8. Seja $\#(T(\varphi))$ o número de nós de $T(\varphi)$. Pelo "número de conectivos em $\varphi$" queremos dizer o número de ocorrências de conectivos em $\varphi$. (Em geral $\#(A)$ designa o número de elementos de um conjunto (finito) $A$).
   (a) Se $\varphi$ não contém $\perp$, demonstre que: o número de conectivos de $\varphi +$ o número de átomos de $\varphi \leq \#(T(\varphi))$.
   (b) $\#(\mathrm{sub}(\varphi)) \leq \#(T(\varphi))$.
   (c) Um ramo de uma árvore é um conjunto maximal linearmente ordenado. O comprimento de um ramo é o número de seus nós menos um. Demonstre que $p(\varphi)$ é o comprimento de um ramo de maior comprimento em $T(\varphi)$.
   (d) Suponha que $\varphi$ não contém $\perp$. Demonstre que: o número de conectivos em $\varphi +$ o número de átomos de $\varphi \leq 2^{p(\varphi)+1} - 1$.

9. Demonstre que uma proposição com $n$ conectivos tem no máximo $2n + 1$ subfórmulas.

10. Demonstre que para $PROP$ temos um teorema de decomposição única: para cada proposição não-atômica $\sigma$ ou existem duas proposições $\varphi$ e $\psi$ tais que $\sigma = \varphi \square \psi$, ou existe uma proposição $\varphi$ tal que $\sigma = \neg\varphi$.

11. (a) Dê uma definição indutiva para a função $F$, definida por recursão sobre $PROP$ a partir das funções $H_{at}$, $H_{\Box}$, $H_{\neg}$, como um conjunto $F^*$ de pares.

    (b) Formule e demonstre para $F^*$ o princípio da indução.

    (c) Demonstre que $F^*$ é de fato uma função sobre $PROP$.

    (d) Demonstre que ela é a única função sobre $PROP$ satisfazendo as equações recursivas.

## 1.2 Semântica

A tarefa de interpretar a lógica proposicional é simplificada pelo fato de que as entidades consideradas têm uma estrutura simples. As proposições são construídas a partir de blocos adicionando-se conectivos.
As partes mais simples (os átomos) são da forma "a grama é verde", "Maria gosta de Goethe", "$6 - 3 = 2$", que são simplesmente *verdadeiras* ou *falsas*. Estendemos essa atribuição de *valores-verdade* a proposições compostas, por reflexão sobre o significado dos conectivos lógicos.

Vamos combinar de usar 1 e 0 ao invés de 'verdadeiro' e 'falso'. O problema que enfrentamos é como interpretar $\varphi \Box \psi$, $\neg\varphi$, dados os valores-verdade de $\varphi$ e $\psi$.

Ilustraremos a solução considerando a tabela entrada-saída para os Srs. Smith e Jones.

*Conjunção.* Um visitante que deseja ver ambos Smith e Jones quer que a tabela esteja na posição mostrada aqui, i.e.

| | entra | sai |
|---|---|---|
| Smith | × | |
| Jones | × | |

"Smith está" $\wedge$ "Jones está" é verdadeiro sse
"Smith está" é verdadeiro e "Jones está" é verdadeiro

Escrevemos $v(\varphi) = 1$ (resp. 0) para "$\varphi$ é verdadeiro". Então a consideração acima pode ser enunciada como sendo $v(\varphi \wedge \psi) = 1$ sse $v(\varphi) = v(\psi) = 1$, ou $v(\varphi \wedge \psi) = \min(v(\varphi), v(\psi))$.

Pode-se também escrever sob forma de uma *tabela-verdade*:

| $\wedge$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

A tabela-verdade deve ser lida da seguinte forma: o primeiro argumento é tomado da coluna mais à esquerda e o segundo argumento é tomado da linha mais acima.

*Disjunção.* Se um visitante deseja ver um dos parceiros, não importa qual, ele deseja que a tabela esteja em uma das posições

| | entra | sai |
|---|---|---|
| Smith | × | |
| Jones | | × |

| | entra | sai |
|---|---|---|
| Smith | | × |
| Jones | × | |

| | entra | sai |
|---|---|---|
| Smith | × | |
| Jones | × | |

No último caso ele pode fazer uma escolha, porém isso não é um problema, pois ele deseja ver pelo menos um dos caras, não importa qual.

Em nossa notação, a interpretação de $\vee$ é dada por

$$v(\varphi \vee \psi) = 1 \qquad \text{sse} \qquad v(\varphi) = 1 \quad \text{ou} \quad v(\psi) = 1$$

Abreviando: $v(\varphi \vee \psi) = \max(v(\varphi), v(\psi))$.

Sob forma de tabela-verdade:

| $\vee$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 1 |

*Negação.* O visitante que está apenas interessado no Sr. Smith enunciará "Smith não está" se a tabela estiver na posição:

| | entra | sai |
|---|---|---|
| Smith | | $\times$ |

Portanto "Smith não está" é verdadeiro se "Smith está" é falso. Escrevemos isso da forma $v(\neg\varphi) = 1$ sse $v(\varphi) = 0$, ou $v(\neg\varphi) = 1 - v(\varphi)$.

Sob forma de tabela-verdade:

| $\neg$ | |
|---|---|
| 0 | 1 |
| 1 | 0 |

*Implicação.* Nosso famoso visitante foi informado de que "Jones está se Smith está". Agora podemos ao menos prever as seguintes posições da tabela

| | entra | sai |
|---|---|---|
| Smith | $\times$ | |
| Jones | $\times$ | |

| | entra | sai |
|---|---|---|
| Smith | | $\times$ |
| Jones | | $\times$ |

Se a tabela está na posição:

| | entra | sai |
|---|---|---|
| Smith | $\times$ | |
| Jones | | $\times$ |

então ele sabe que a informação era falsa.

O caso remanescente,

| | entra | sai |
|---|---|---|
| Smith | | $\times$ |
| Jones | $\times$ | |

, não pode ser tratado de forma tão simples. Evidentemente não há razão para considerar a informação falsa, mas sim que "não ajuda muito", ou "irrelevante". Entretanto, nos comprometemos com a posição de que cada enunciado é verdadeiro ou falso, por isso temos que decidir atribuir a "Se Smith está, então Jones está" verdadeiro também nesse caso particular. O leitor vai se dar conta de que fizemos uma escolha deliberada aqui; uma escolha que se revelará uma escolha feliz em vista da elegância do sistema resultante. Não há razão convincente, entretanto, para se permanecer com a noção de implicação que acabamos de introduzir. Embora várias outras noções tenham sido estudadas na literatura, para propósitos matemáticos nossa noção é perfeitamente apropriada.

Note que há um caso em que a implicação é falsa (veja a tabela-verdade abaixo), e vamos manter essa observação na lembrança para aplicação mais adiante – ela vai ajudar a diminuir os cálculos.

Em nossa notação a interpretação da implicação é dada por $v(\varphi \to \psi) = 0$ sse $v(\varphi) = 1$ e $v(\psi) = 0$.

Sua tabela-verdade é:

| $\to$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 0 | 1 |

*Equivalência.* Se nosso visitante sabe que "Smith está se e somente se Jones está", então ele sabe que ambos estão presentes ou ambos não estão. Logo $v(\varphi \to \psi) = 1$ sse $v(\varphi) = v(\psi)$.

Sua tabela-verdade é:

| $\leftrightarrow$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 0 | 1 |

*Falsum.* Um absurdo, tal como "$0 \neq 0$", "alguns números ímpares são pares", "Eu não sou eu", não podem ser verdadeiros. Logo colocamos $v(\bot) = 0$.

Estritamente falando deveríamos adicionar uma tabela-verdade, i.e. a tabela para $\top$, o oposto de *falsum*.

*Verum.* Esse símbolo designa proposições evidentemente verdadeiras tal como $1 = 1$; colocamos $v(\top) = 1$ para todo $v$.

**Definição 1.2.1** Um mapeamento $v : PROP \to \{0,1\}$ é uma *valoração* se

$$\begin{array}{lll}
v(\varphi \wedge \psi) & = & \min(v(\varphi), v(\psi)), \\
v(\varphi \vee \psi) & = & \max(v(\varphi), v(\psi)), \\
v(\varphi \to \psi) & = & 0 \quad \Leftrightarrow \quad v(\varphi) = 1 \text{ e } v(\psi) = 0, \\
v(\varphi \leftrightarrow \psi) & = & 1 \quad \Leftrightarrow \quad v(\varphi) = v(\psi), \\
v(\neg\varphi) & = & 1 - v(\varphi), \\
v(\bot) & = & 0.
\end{array}$$

Se uma valoração é dada apenas para átomos então, em virtude da definição por recursão, é possível extendê-la para todas as proposições, portanto obtemos:

**Teorema 1.2.2** *Se $v$ é um mapeamento do conjunto de átomos em $\{0,1\}$, satisfazendo $v(\bot) = 0$, então existe uma única valoração $[\![\cdot]\!]_v$, tal que $[\![\varphi]\!]_v = v(\varphi)$ para $\varphi$ atômica.*

Tem sido prática comum designar valorações como definidas acima por $[\![\varphi]\!]$, por isso adotaremos essa notação. Como $[\![\cdot]\!]$ é completamente determinado por seus valores sobre os átomos, $[\![\varphi]\!]$ é frequentemente designado por $[\![\varphi]\!]_v$. Sempre que não houver confusão omitiremos o índice $v$.

O teorema 1.2.2 nos diz que cada um dos mapeamentos $v$ e $[\![\cdot]\!]_v$ determina o outro de forma única, por conseguinte chamamos $v$ também de valoração (ou de uma *valoração atômica*, se necessário). Desse teorema torna-se aparente que existem muitas valorações (cf. Exercício 4).

É óbvio também que o *valor* $[\![\varphi]\!]_v$ *de* $\varphi$ *sob* $v$ somente depende dos valores de $v$ nas suas subfórmulas atômicas:

**Lema 1.2.3** *Se $v(p_i) = v'(p_i)$ para todo $p_i$ ocorrendo em $\varphi$, então $[\![\varphi]\!]_v = [\![\varphi]\!]_{v'}$.*

*Demonstração.* Uma indução fácil sobre $\varphi$.

Um importante subconjunto de $PROP$ é o de todas as proposições $\varphi$ que são *sempre verdadeiras*, i.e. verdadeiras sob todas as valorações.

**Definição 1.2.4** (i) $\varphi$ é uma *tautologia* se $[\![\varphi]\!]_v = 1$ para todas as valorações $v$,
(ii) $\models \varphi$ designa '$\varphi$ é uma tautologia',
(iii) Seja $\Gamma$ um conjunto de proposições, então $\Gamma \models \varphi$ sse para todo $v$: ($[\![\psi]\!]_v = 1$ para todo $\psi \in \Gamma$) $\Rightarrow [\![\varphi]\!]_v = 1$.

Em palavras, $\Gamma \models \varphi$ se verifica sse $\varphi$ é verdadeira sob toda valoração que torna toda fórmula $\psi$ em $\Gamma$ verdadeira. Dizemos que $\varphi$ é uma conseqüência semântica de $\Gamma$. Escrevemos $\Gamma \not\models \varphi$ se $\Gamma \models \varphi$ não é o caso.

*Convenção.* $\varphi_1, \ldots, \varphi_n \models \psi$ designa $\{\varphi_1, \ldots, \varphi_n\} \models \psi$.

Note que "$[\![\varphi]\!]_v = 1$ para toda $v$" é uma outra maneira de dizer "$[\![\varphi]\!] = 1$ para todas as valorações".

*Exemplos.* (i) $\models \varphi \to \varphi$; $\models \neg\neg\varphi \to \varphi$; $\models \varphi \vee \psi \leftrightarrow \psi \vee \varphi$,
(ii) $\varphi, \psi \models \varphi \wedge \psi$; $\varphi, \varphi \to \psi \models \psi$; $\varphi \to \psi, \neg\psi \models \neg\varphi$.

Frequentemente se precisa de substituir subfórmulas por proposições; acontece que basta definir substituição apenas para átomos.

Escrevemos $\varphi[\psi/p_i]$ para designar a proposição obtida substituindo-se todas as ocorrências de $p_i$ em $\varphi$ por $\psi$. Na realidade, a substituição de $p_i$ por $\psi$ define um mapeamento de $PROP$ em $PROP$, que pode ser dado por recursão (sobre $\varphi$).

**Definição 1.2.5**

$$\begin{array}{lcl}
\varphi[\psi/p_i] & = & \begin{cases} \varphi & \textit{se } \varphi \textit{ atômica e } \varphi \neq p_i \\ \psi & \textit{se } \varphi = p_i \end{cases} \\
(\varphi_1 \Box \varphi_2)[\psi/p_i] & = & \varphi_1[\psi/p_i] \Box \varphi_2[\psi/p_i] \\
(\neg\varphi)[\psi/p_i] & = & \neg\varphi[\psi/p_i].
\end{array}$$

O teorema seguinte expõe as propriedades básicas da substituição de proposições equivalentes.

**Teorema 1.2.6 (Teorema da Substituição)** *Se* $\models \varphi_1 \leftrightarrow \varphi_2$*, então* $\models \psi[\varphi_1/p] \leftrightarrow \psi[\varphi_2/p]$*, onde* $p$ *é um átomo.*

O teorema da substituição é na verdade uma conseqüência de um lema um pouco mais forte

**Lema 1.2.7** $[\![\varphi_1 \leftrightarrow \varphi_2]\!]_v \leq [\![\psi[\varphi_1/p] \leftrightarrow \psi[\varphi_2/p]]\!]_v$ *e*
$\models (\varphi_1 \leftrightarrow \varphi_2) \to (\psi[\varphi_1/p] \leftrightarrow \psi[\varphi_2/p])$

*Demonstração.* Indução sobre $\varphi$. Apenas temos que considerar $[\![\varphi_1 \leftrightarrow \varphi_2]\!]_v = 1$ (por que?).

- $\psi$ atômica. Se $\psi = p$, então $\psi[\varphi_i/[] = \varphi_i$ e o resultado segue imediatamente. Se $\psi \neq p$, então $\psi[\varphi_i/p] = \psi$, e $[\![\psi[\varphi_1/p] \leftrightarrow \psi[\varphi_2/p]]\!]_v = [\![\psi \leftrightarrow \psi]\!]_v = 1$.
- $\psi = \psi_1 \Box \psi_2$. Hipótese da indução: $[\![\psi_i[\varphi_1/p]]\!]_v = [\![\psi_i[\varphi_2/p]]\!]_v$. Agora o valor de $[\![(\psi_1 \Box \psi_2)[\varphi_i/p]]\!]_v = [\![\psi_1[\varphi_i/p] \Box \psi_2[\varphi_i/p]]\!]_v$ é unicamente determinado por suas partes $[\![\psi_j[\varphi_i/p]]\!]_v$, logo $[\![(\psi_1 \Box \psi_2)[\varphi_1/p]]\!]_v = [\![(\psi_1 \Box \psi_2)[\varphi_2/p]]\!]_v$.

– $\psi = \neg\psi_1$. Deixo para o leitor.

A prova da segunda parte essencialmente usa o fato de que $\models \varphi \to \psi$ sse $[\![\varphi]\!]_v \leq [\![\psi]\!]_v$ para toda $v$ (cf. Exercício 6). □

A prova do teorema da substituição agora segue imediatamente. □

O teorema da substituição diz em bom português que *partes podem ser substituídas por partes equivalentes*.

Existem várias técnicas para se testar tautologias. Uma delas (bastante lenta) usa tabelas-verdade. Damos um exemplo:

$$(\varphi \to \psi) \leftrightarrow (\neg\psi\neg\varphi)$$

| $\varphi$ | $\psi$ | $\neg\varphi$ | $\neg\psi$ | $\varphi \to \psi$ | $\neg\psi \to \neg\varphi$ | $(\varphi \to \psi) \leftrightarrow (\neg\psi \to \neg\varphi)$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 1 | 1 | 0 | 0 | 1 | 1 | 1 |

A última coluna consiste de 1's apenas. Como, pelo lema 1.2.3 apenas os valores de $\varphi$ e $\psi$ são relevantes, tivemos que testar $2^2$ casos. Se existirem $n$ partes (atômicas) precisamos de $2^n$ linhas.

Podemos comprimir um pouco a tabela acima, escrevendo-a da seguinte forma:

| $(\varphi$ | $\to$ | $\psi)$ | $\leftrightarrow$ | $(\neg\psi$ | $\to$ | $\neg\varphi)$ |
|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 0 |

Vamos fazer uma outra observação sobre o papel dos conectivos 0-ários $\bot$ e $\top$. Claramente $\models \top \leftrightarrow (\bot \to \bot)$, logo podemos definir $\top$ a partir de $\bot$. Por outro lado, não podemos definir $\bot$ a partir de $\top$ e $\to$; note que a partir de $\top$ nunca podemos obter algo exceto uma proposição equivalente a $\top$ se usamos $\wedge$, $\vee$, $\to$, mas a partir de $\bot$ podemos gerar $\bot$ e $\top$ através da aplicação de $\wedge$, $\vee$, $\to$.

## Exercícios

1. Verifique pelo método da tabela-verdade quais das seguintes proposições são tautologias:
   (a) $(\neg\varphi \vee \psi) \leftrightarrow (\psi \to \varphi)$
   (b) $\varphi \to ((\psi \to \sigma) \to ((\varphi \to \psi) \to (\varphi \to \sigma)))$
   (c) $(\varphi \to \neg\varphi) \leftrightarrow \neg\varphi$
   (d) $\neg(\varphi \to \neg\varphi)$
   (e) $(\varphi \to (\psi \to \sigma)) \leftrightarrow ((\varphi \wedge \psi) \to \sigma)$
   (f) $\varphi \vee \neg\varphi$ (*princípio do terceiro excluído*)
   (g) $\bot \leftrightarrow (\varphi \wedge \neg\varphi)$
   (h) $\bot \to \varphi$ (*ex falso sequitur quodlibet*)

2. Demonstre que: (a) $\varphi \models \varphi$;

   (b) $\varphi \models \psi$ e $\psi \models \sigma \Rightarrow \varphi \models \sigma$;

   (c) $\models \varphi \to \psi \Leftrightarrow \varphi \models \psi$.

3. Determine $\varphi[\neg p_0 \to p_3/p_0]$ para $\varphi = p_1 \wedge p_0 \to (p_0 \to p_3)$;

   $\varphi = (p_3 \leftrightarrow p_0) \vee (p_2 \to \neg p_0)$.

4. Demonstre que existem $2^{\aleph_0}$ valorações.

5. Demonstre que $[\![\varphi \wedge \psi]\!]_v = [\![\varphi]\!]_v \cdot [\![\psi]\!]_v$,

   $[\![\varphi \vee \psi]\!]_v = [\![\varphi]\!]_v + [\![\psi]\!]_v - [\![\varphi]\!]_v \cdot [\![\psi]\!]_v$,

   $[\![\varphi \to \psi]\!]_v = 1 - [\![\varphi]\!]_v + [\![\varphi]\!]_v \cdot [\![\psi]\!]_v$,

   $[\![\varphi \leftrightarrow \psi]\!]_v = 1 - |[\![\varphi]\!]_v - [\![\psi]\!]_v|$.

6. Demonstre que $[\![\varphi \to \psi]\!]_v = 1 \quad \Leftrightarrow \quad [\![\varphi]\!]_v \leq [\![\psi]\!]_v$.

## 1.3 Algumas Propriedades da Lógica Proposicional

Com base nas seções anteriores já podemos provar muitos teoremas sobre a lógica proposicional. Uma das primeiras descobertas na lógica proposicional moderna foi sua semelhança com álgebras.
Após Boole, um estudo amplo das propriedades algébricas foi realizado por muitos lógicos. Os aspectos puramente algébricos têm desde então sido estudados na chamada *Álgebra de Boole*.

Apenas mencionaremos um pequeno número dessas leis algébricas.

**Teorema 1.3.1** *As seguintes proposições são tautologias.*

$$(\varphi \vee \psi) \vee \sigma \leftrightarrow \varphi \vee (\psi \vee \sigma) \quad (\varphi \vee \psi) \wedge \sigma \leftrightarrow \varphi \wedge (\psi \wedge \sigma)$$
*associatividade*
$$\varphi \vee \psi \leftrightarrow \psi \vee \varphi \quad \varphi \wedge \psi \leftrightarrow \psi \wedge \varphi$$
*comutatividade*
$$\varphi \vee (\psi \wedge \sigma) \leftrightarrow (\varphi \vee \psi) \wedge (\varphi \vee \sigma) \quad \varphi \wedge (\psi \vee \sigma) \leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \sigma)$$
*distributividade*
$$\neg(\varphi \vee \psi) \leftrightarrow \neg\varphi \wedge \neg\psi \quad \neg(\varphi \wedge \psi) \leftrightarrow \neg\varphi \vee \neg\psi$$
*leis de De Morgan*
$$\varphi \vee \varphi \leftrightarrow \varphi \quad \varphi \wedge \varphi \leftrightarrow \varphi$$
*idempotência*
$$\neg\neg\varphi \leftrightarrow \varphi$$
*lei da dupla negação*

*Demonstração*. Verifique a tabela verdade ou faça alguns cálculos. E.g. a lei de De Morgan: $[\![\neg(\varphi \vee \psi)]\!] = 1 \Leftrightarrow [\![\varphi \vee \psi]\!] = 0 \Leftrightarrow [\![\varphi]\!] = [\![\psi]\!] = 0 \Leftrightarrow [\![\neg\varphi]\!] = [\![\neg\psi]\!] = 1 \Leftrightarrow [\![\neg\varphi \wedge \neg\psi]\!] = 1$.
Logo $[\![\neg(\varphi \vee \psi)]\!] = [\![\neg\varphi \wedge \psi]\!]$ para todas as valorações, i.e. $\models \neg(\varphi \vee \psi) \leftrightarrow \neg\varphi \wedge \neg\psi$.
As tautologias restantes são deixadas ao leitor. $\square$

Para aplicar o teorema anterior em "cálculos lógicos" precisamos de mais algumas equivalências. Isso é demonstrado na simples equivalência $\models \varphi \wedge (\varphi \vee \psi) \leftrightarrow \varphi$ (exercício para o leitor). Pois, pela lei da distributividade $\models \varphi \wedge (\varphi \vee \psi) \leftrightarrow (\varphi \wedge \varphi) \vee (\varphi \wedge \psi)$ e $\models (\varphi \wedge \varphi) \vee (\varphi \wedge \psi) \leftrightarrow \varphi \vee (\varphi \wedge \psi)$, por idempotência e pelo teorema da substituição. Logo $\models \varphi \wedge (\varphi \vee \psi) \leftrightarrow \varphi \vee (\varphi \wedge \psi)$. Uma outra aplicação da lei da distributividade nos levará de volta ao início, portanto apenas aplicando-se as leis acima não nos permitirá eliminar $\psi$!

Listamos portanto mais algumas propriedades convenientes.

**Lema 1.3.2**
*Se* $\models \varphi \rightarrow \psi$, *então* $\models \varphi \wedge \psi \leftrightarrow \varphi$
$\models \varphi \vee \psi \leftrightarrow \psi$

*Demonstração.* Pelo Exercício 6 da seção 1.2 $\models \varphi \rightarrow \psi$ implica que $[\![\varphi]\!]_v \leq [\![\psi]\!]_v$ para toda valoração $v$. Logo $[\![\varphi \wedge \psi]\!]_v = \min([\![\varphi]\!]_v, [\![\psi]\!]_v) = [\![\varphi]\!]_v$ e $[\![\varphi \vee \psi]\!]_v = \max([\![\varphi]\!]_v, [\![\psi]\!]_v) = [\![\psi]\!]_v$ para toda $v$. □

**Lema 1.3.3**
(a) $\models \varphi \quad \Rightarrow \quad \models \varphi \wedge \psi \leftrightarrow \psi$
(b) $\models \varphi \quad \Rightarrow \quad \models \neg\varphi \vee \psi \leftrightarrow \psi$
(c) $\models \bot \vee \psi \leftrightarrow \psi$
(d) $\models \top \wedge \psi \leftrightarrow \psi$

*Demonstração.* Deixo ao leitor. □

O teorema a seguir estabelece algumas equivalências envolvendo vários conectivos. Ele nos diz que podemos "definir" a menos de equivalência lógica todos os conectivos em termos de $\{\vee, \neg\}$, ou $\{\rightarrow, \neg\}$, ou $\{\wedge, \neg\}$, ou $\{\rightarrow, \bot\}$.
Ou seja, podemos encontrar e.g. uma proposição envolvendo apenas $\vee$ e $\neg$, que é equivalente a $\varphi \leftrightarrow \psi$, etc.

**Teorema 1.3.4**
(a) $\models (\varphi \leftrightarrow \psi) \leftrightarrow (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$,
(b) $\models (\varphi \rightarrow \psi) \leftrightarrow (\neg\varphi \vee \psi)$,
(c) $\models \varphi \vee \psi \leftrightarrow (\neg\varphi \rightarrow \psi)$,
(d) $\models \varphi \vee \psi \leftrightarrow \neg(\neg\varphi \wedge \neg\psi)$,
(e) $\models \varphi \wedge \psi \leftrightarrow \neg(\neg\varphi \vee \neg\psi)$,
(f) $\models \neg\varphi \leftrightarrow (\varphi \rightarrow \bot)$,
(g) $\models \bot \leftrightarrow \varphi \wedge \neg\varphi$.

*Demonstração.* Calcule os valores-verdade das proposições à esquerda e das proposições à direita. □

Agora temos material suficiente para lidar com lógica como se fosse álgebra. Por conveniência escrevemos $\varphi \approx \psi$ para designar $\models \varphi \leftrightarrow \psi$.

**Lema 1.3.5**
$\approx$ *é uma relação de equivalência sobre* $PROP$, *i.e.*
$\varphi \approx \varphi$ (*reflexividade*),
$\varphi \approx \psi \quad \Rightarrow \quad \psi \approx \varphi$ (*simetria*),
$\varphi \approx \psi$ *e* $\psi \approx \sigma \quad \Rightarrow \quad \varphi \approx \sigma$ (*transitividade*).

*Demonstração.* Use $\models \varphi \leftrightarrow \psi$ sse $[\![\varphi]\!]_v = [\![\psi]\!]_v$ para toda $v$. □

Vamos dar alguns exemplos de cálculos algébricos que estabelecem uma cadeia de equivalências.

1. $\models (\varphi \to (\psi \to \sigma)) \leftrightarrow (\varphi \wedge \psi \to \sigma)$,

$$\begin{array}{rcll} \varphi \to (\psi \to \sigma) & \approx & \neg\varphi \vee (\psi \to \sigma), & (1.3.4(b)) \\ \neg\varphi \vee (\psi \to \sigma) & \approx & \neg\varphi \vee (\neg\psi \vee \sigma), & (1.3.4(b) \text{ e teor. subst.}) \\ \neg\varphi \vee (\neg\psi \vee \sigma) & \approx & (\neg\varphi \vee \neg\psi) \vee \sigma, & (\text{associatividade}) \\ (\neg\varphi \vee \neg\psi) \vee \sigma & \approx & \neg(\varphi \wedge \psi) \vee \sigma & (\text{De Morgan e teor. subst.}) \\ \neg(\varphi \wedge \psi) \vee \sigma & \approx & (\varphi \wedge \psi) \to \sigma, & (1.3.4(b)) \\ \text{Logo } \varphi \to (\psi \to \sigma) & \approx & (\varphi \wedge \psi) \to \sigma. & \end{array}$$

   Agora deixamos de fora as referências aos fatos utilizados, e formamos uma longa cadeia. Basta calcular até atingirmos uma tautologia.

2. $\models (\varphi \to \psi) \leftrightarrow (\neg\psi \to \neg\varphi)$,

   $\neg\psi \to \neg\varphi \approx \neg\neg\psi \vee \neg\varphi \approx \psi \vee \neg\varphi \approx \neg\varphi \vee \psi \approx \varphi \to \psi$

3. $\models \varphi \to (\psi \to \varphi)$,

   $\varphi \to (\psi \to \varphi) \approx \neg\varphi \vee (\neg\psi \vee \varphi) \approx (\neg\varphi \vee \varphi) \vee \neg\psi$.

Vimos que $\vee$ e $\wedge$ são associativos, porisso adotamos a convenção, também usada em álgebra, de omitir parênteses em disjunções e conjunções iteradas; ou seja, escrevemos $\varphi_1 \vee \varphi_2 \vee \varphi_3 \vee \varphi_4$, etc. Isso é correto, pois independentemente da forma como recuperarmos (corretamente do ponto de vista sintático) os parênteses, a fórmula resultante é determinada unicamente a menos de equivalência.

Será que até esse ponto introduzimos *todos* os conectivos? Obviamente não. Podemos facilmente inventar novos conectivos. Aqui vai um famoso, introduzido por Sheffer: $\varphi|\psi$ designa "não é verdade que ambos $\varphi$ e $\psi$ são verdadeiros". Mais precisamente: $\varphi|\psi$ é dado pela seguinte tabela-verdade:

*barra de Sheffer*

| \| | 0 | 1 |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 1 | 0 |

Vamos dizer que um conectivo lógico $n$-ário \$ é *definido* por sua tabela-verdade, ou por sua função de avaliação, se $[\![\$(p_1,\ldots,p_n)]\!] = f([\![p_1]\!],\ldots,[\![p_n]\!])$ para alguma função $f$.
Embora possamos aparentemente introduzir muitos conectivos novos dessa forma, não há surpresas em estoque nos esperando, pois todos aqueles conectivos são definíveis em termos de $\vee$ e $\neg$:

**Teorema 1.3.6** *Para cada conectivo $n$-ário \$ definido por sua função de avaliação, existe uma proposição $\tau$, contendo apenas $p_1,\ldots,p_n$, $\vee$ e $\neg$, tal que $\models \tau \leftrightarrow \$(p_1,\ldots,p_n)$.*

*Demonstração.* Por indução sobre $n$. Para $n = 1$ existem 4 conectivos possíveis com tabelas-verdade

| $\$_1$ | |
|---|---|
| 0 | 0 |
| 1 | 0 |

| $\$_2$ | |
|---|---|
| 0 | 1 |
| 1 | 1 |

| $\$_3$ | |
|---|---|
| 0 | 0 |
| 1 | 1 |

| $\$_4$ | |
|---|---|
| 0 | 1 |
| 1 | 0 |

Facilmente se verifica que todas as proposições $\neg(p \vee \neg p)$, $p \vee \neg p$, $p$ e $\neg p$ atenderão aos requisitos.

Suponha que para todos os conectivos $n$-ários foram encontradas as proposições. Considere $\$(p_1, \ldots, p_n, p_{n+1})$ com a tabela-verdade:

| $p_1$ | $p_2$ | $\ldots$ | $p_n$ | $p_{n+1}$ | $\$(p_1, \ldots, p_n, p_{n+1})$ |
|---|---|---|---|---|---|
| 0 | 0 | | 0 | 0 | $i_1$ |
| . | . | | 0 | 1 | $i_2$ |
| . | 0 | | 1 | . | . |
| . | 1 | | 1 | . | . |
| 0 | . | | . | . | . |
| . | 1 | | . | . | . |
| ... | ... | ... | ... | ... | ... |
| 1 | 0 | | . | . | . |
| . | . | | . | . | . |
| . | . | | . | . | . |
| . | 0 | | . | . | . |
| . | 1 | | 0 | . | . |
| . | . | | 0 | . | . |
| 1 | . | | 1 | 0 | . |
| . | . | | 1 | 1 | $i_{2^{n+1}}$ |

onde $i_k \leq 1$.

Consideramos dois conectivos auxiliares $\$_1$ e $\$_2$ definidos por

$\$_1(p_2, \ldots, p_{n+1}) = \$(\bot, p_2, \ldots, p_{n+1})$ e
$\$_2(p_2, \ldots, p_{n+1}) = \$(\top, p_2, \ldots, p_{n+1})$ onde $\top = \neg\bot$

(como foi dado pelas metades superior e inferior da tabela acima).

Pela hipótese da indução existem proposições $\sigma_1$ e $\sigma_2$, contendo apenas $p_1, \ldots, p_{n+1}$, $\vee$ e $\neg$ tal que $\models \$_i(p_2, \ldots, p_{n+1}) \leftrightarrow \sigma_i$.
A partir daquelas duas proposições podemos construir a proposição $\tau$:
$\tau := (p_1 \to p_2) \wedge (\neg p_1 \to \sigma_1)$.

*Alegação* $\models \$(p_1, \ldots, p_{n+1}) \leftrightarrow \tau$.

Se $[\![p_1]\!]_v = 0$ então $[\![p_1 \to \sigma_2]\!]_v = 1$, logo $[\![\tau]\!]_v = [\![\neg p_1 \to \sigma_1]\!]_v = [\![\sigma_1]\!]_v = [\![\$_1(p_2, \ldots, p_{n+1})]\!]_v = [\![\$(p_1, p_2, \ldots, p_{n+1})]\!]_v$, usando $[\![p_1]\!]_v = 0 = [\![\bot]\!]_v$.

O caso $[\![p_1]\!]_v = 1$ é semelhante.

Agora exprimindo $\to$ e $\wedge$ em termos de $\vee$ e $\neg$ (1.3.4), temos $[\![\tau']\!] = [\![\$(p_1, \ldots, p_{n+1})]\!]$ para todas as valorações (um outro uso do lema 1.2.3), onde $\tau' \approx \tau$ e $\tau'$ contém apenas os conectivos $\vee$ e $\neg$. $\square$

Para uma outra solução veja o Exercício 7.

O teorema acima e o teorema 1.3.4 são justificações pragmáticas para nossa escolha da tabela-verdade para $\to$: obtemos uma teoria extremamente elegante e útil. O teorema 1.3.6 é usualmente expresso dizendo-se que $\vee$ e $\neg$ formam um conjunto *funcionalmente completo* de conectivos. Igualmente $\wedge$, $\neg$ e $\to$, $\neg$ e $\bot$, $\to$ formam conjuntos funcionalmente completos.

Por analogia com $\sum$ e $\prod$ de álgebra, introduzimos disjunções e conjunções finitas:

**Definição 1.3.7**

$$\begin{cases} \bigwedge\limits_{i\leq 0}\varphi_i & = \varphi_0 \\ \bigwedge\limits_{i\leq n+1}\varphi_i & = \bigwedge\limits_{i\leq n}\varphi_i \wedge \varphi_{n+1} \end{cases} \qquad \begin{cases} \bigvee\limits_{i\leq 0}\varphi_i & = \varphi_0 \\ \bigvee\limits_{i\leq n+1}\varphi_i & = \bigvee\limits_{i\leq n}\varphi_i \vee \varphi_{n+1} \end{cases}$$

**Definição 1.3.8** *Se* $\varphi = \bigwedge\limits_{i\leq n}\bigvee\limits_{j\leq m_i}\varphi_{ij}$*, onde* $\varphi_{ij}$ *é atômica ou a negação de um átomo, então* $\varphi$ *é uma* forma normal conjuntiva. *Se* $\varphi = \bigvee\limits_{i\leq n}\bigwedge\limits_{j\leq m_i}\varphi_{ij}$*, onde* $\varphi_{ij}$ *é atômica ou a negação de um átomo, então* $\varphi$ *é uma* forma normal disjuntiva.

As formas normais são análogas às bem-conhecidas formas normais em álgebra: $ax^2 + byx$ é "normal", enquanto que $x(ax + by)$ não é. Pode-se obter formas normais simplesmente "multiplicando", i.e. aplicação repetida de leis distributivas. Em álgebra existe apenas uma "forma normal"; em lógica existe uma certa dualidade entre $\wedge$ e $\vee$, de tal forma que temos dois teoremas da forma normal.

**Teorema 1.3.9** *Para cada* $\varphi$ *existem as formas normais conjuntivas* $\varphi^\wedge$ *e as formas normais disjuntivas* $\varphi^\vee$*, tais que* $\models \varphi \leftrightarrow \varphi^\wedge$ *e* $\models \varphi \leftrightarrow \varphi^\vee$.

*Demonstração.* Primeiro elimine todos os conectivos exceto $\perp$, $\wedge$, $\vee$ e $\neg$. Então demonstre o teorema por indução sobre a proposição resultante na linguagem restrita a $\perp$, $\wedge$, $\vee$ e $\neg$. Na verdade $\perp$ não tem qualquer papel nesse cenário; poderia muito bem ser ignorado.

(a) $\varphi$ é atômica. Então $\varphi^\wedge = \varphi^\vee = \varphi$.

(b) $\varphi = \psi \wedge \sigma$. Então $\varphi^\wedge = \psi^\wedge \wedge \sigma^l and$.

Para obter uma forma normal disjuntiva consideramos $\psi^\vee = \bigvee \psi_i$, $\sigma^\vee = \bigvee \sigma_j$, onde os $\psi_i$'s e os $\sigma_j$'s são conjunções de átomos e negações de átomos.

Agora $\varphi = \psi \wedge \sigma \approx \psi^\vee \wedge \sigma^\vee \approx \bigvee\limits_{i,j}(\psi_i \wedge \sigma_j)$.

A última proposição está na forma normal, logo dizemos que $\varphi^\vee$ é essa fórmula.

(c) $\varphi = \psi \wedge \sigma$. Semelhante a (b).

(d) $\varphi = \neg\psi$. Por hipótese da indução $\psi$ tem formas normais $\psi^\vee$ e $\psi^\wedge$.

$\neg\psi \approx \neg\psi^\wedge \approx \neg\bigvee\bigwedge\psi_{i,j} \approx \bigwedge\bigvee\neg\psi_{i,j} \approx \bigwedge\bigvee\psi'_{i,j}$, onde $\psi'_{i,j} = \neg\psi_{i,j}$ se $\psi_{i,j}$ é atômica, e $\psi_{i,j} = \neg\psi'_{i,j}$ se $\psi_{i,j}$ é a negação de um átomo. (Observe que $\neg\neg\psi_{i,j} \approx \psi_{i,j}$.) Claramente $\bigwedge\bigvee\psi'_{i,j}$ está na forma normal conjuntiva para $\varphi$. A forma normal disjuntiva é deixada para o leitor.

Para uma outra demonstração dos teoremas da forma normal veja Exercício 7. □

Olhando para a álgebra da lógica no teorema 1.3.1, vimos que $\vee$ e $\wedge$ se comportaram de uma maneira semelhante, a ponto de que as mesmas leis se verificam para ambos. Vamos tornar essa 'dualidade' mais precisa. Para esse propósito consideramos uma linguagem com apenas os conectivos $\vee$, $\wedge$ e $\neg$.

**Definição 1.3.10** Defina um mapeamento auxiliar $*: PROP \to PROP$ recursivamente da seguinte forma

$$\begin{array}{rcl} \varphi^* & = & \neg\varphi \text{ se } \varphi \text{ é atômica}, \\ (\varphi \wedge \psi)^* & = & \varphi^* \vee \psi^*, \\ (\varphi \vee \psi)^* & = & \varphi^* \wedge \psi^*, \\ (\neg\varphi)^* & = & \neg\varphi^*. \end{array}$$

*Exemplo.* $((p_0 \wedge \neg p_1) \vee p_2)^* = (p_0 \wedge \neg p_1)^* \wedge p_2^* = (p_0^* \vee (\neg p_1)^*) \wedge \neg p_2 = (\neg p_0 \vee \neg p_1^*) \wedge \neg p_2 = (\neg p_0 \vee \neg\neg p_1) \wedge \neg p_2 \approx (\neg p_0 \vee p_1) \wedge \neg p_2$.

Note que o efeito da tradução "$*$" resume-se a tomar a negação e aplicar as leis de De Morgan.

**Lema 1.3.11** $[\![\varphi^*]\!] = [\![\neg\varphi]\!]$.

*Demonstração.* Indução sobre $\varphi$. Para $\varphi$ atômica $[\![\varphi^*]\!] = [\![\neg\varphi]\!]$.
$[\![(\varphi \wedge \psi)^*]\!] = [\![\varphi^* \vee \psi^*]\!] = [\![\neg\varphi \vee \neg\psi]\!] = [\![\neg(\varphi \wedge \psi)]\!]$.
$[\![(\varphi \vee \psi)^*]\!]$ e $[\![(\neg\varphi)^*]\!]$ são deixados ao leitor. □

**Corolário 1.3.12** $\models \varphi^* \leftrightarrow \neg\varphi$.

*Demonstração.* Imediata do Lema 1.3.11. □

Até agora não é bem a dualidade que procuramos. Na verdade desejamos apenas intercambiar $\wedge$ e $\vee$. Por isso introduzimos uma nova função de tradução.

**Definição 1.3.13** A função de tradução $^d : PROP \to PROP$ é recursivamente definida por

$$\begin{array}{rcl} \varphi^d & = & \varphi \text{ para } \varphi \text{ atômica}, \\ (\varphi \wedge \psi)^d & = & \varphi^d \vee \psi^d, \\ (\varphi \vee \psi)^d & = & \varphi^d \wedge \varphi^d, \\ (\neg\varphi)^d & = & \neg\varphi^d. \end{array}$$

**Teorema 1.3.14 (Teorema da Dualidade)** $\models \varphi \leftrightarrow \varphi\psi \;\Leftrightarrow\; \models \varphi^d \leftrightarrow \psi^d$.

*Demonstração.* Usamos a tradução "$*$" como um passo intermediário. Vamos introduzir a noção de substituição simultânea para simplificar a demonstração: $\sigma[\tau_o, \ldots, \tau_n/p_0, \ldots, p_n]$ é obtida substituindo-se $p_i$ por $\tau_i$ para todo $i \le n$ simultaneamente (veja Exercício 15). Observe que $\varphi^* = \varphi^d[\neg p_0, \ldots, \neg p_n]$, logo $\varphi^*[\neg p_0, \ldots, \neg p_n] = \varphi^d[\neg\neg p_0, \ldots, \neg\neg p_n/p_0, \ldots, p_n]$, onde os átomos de $\varphi$ ocorrem entre $p_0, \ldots, p_n$.

Pelo Teorema da Substituição $\models \varphi^d \leftrightarrow \varphi^*[\neg p_o, \ldots, \neg p_n/p_0, \ldots, p_n]$. A mesma equivalência se verifica para $\psi$.

Pelo Corolário 1.3.12 $\models \varphi^* \leftrightarrow \neg\varphi$, $\models \psi^* \leftrightarrow \neg\psi$. Como $\models \varphi \leftrightarrow \psi$, temos também $\models \neg\varphi \leftrightarrow \neg\psi$. Logo $\models \varphi^* \leftrightarrow \psi^*$, e portanto $\models \varphi^*[\neg p_0, \ldots, \neg p_n/p_0, \ldots, p_n] \leftrightarrow \varphi^*[\neg p_0, \ldots, \neg p_n]/p_0, \ldots, p_n]$.

Usando a relação acima entre $\varphi^d$ e $\varphi^*$ obtemos $\models \varphi^d \leftrightarrow \psi^d$. A recíproca segue imediatamente, pois $\varphi^{dd} = \varphi$. □

O Teorema da Dualidade nos dá gratuitamente uma identidade para cada identidade que estabelecemos.

**Exercícios**

1. Demonstre por meios 'algébricos'

   $\models \quad (\varphi \to \psi) \leftrightarrow (\neg\psi \to \neg\varphi)$, *Contraposição*,

   $\models \quad (\varphi \to \psi) \wedge (\psi \to \sigma) \to (\varphi \to \sigma)$, *transitividade da* $\to$,

   $\models \quad (\varphi \to (\psi \wedge \neg\psi)) \to \neg\varphi$,

   $\models \quad (\varphi \to \neg\varphi) \to \neg\varphi$,

   $\models \quad \neg(\varphi \wedge \neg\varphi)$,

   $\models \quad \varphi \to (\psi \to \varphi \wedge \psi)$,

   $\models \quad ((\varphi \to \psi) \to \varphi) \to \varphi$. *Lei de Peirce.*

2. Simplifique as seguintes proposições (i.e. encontre uma proposição equivalente mais simples).

   (a) $(\varphi \to \psi) \wedge \varphi$, (b) $(\varphi\psi) \vee \neg\varphi$ (c) $(\varphi \to \psi) \to \psi$,
   (d) $\varphi \to (\varphi \wedge \psi)$, (e) $(\varphi \wedge \psi) \vee \varphi$, (f) $(\varphi \to \psi) \to \varphi$

3. Mostre que $\{\neg\}$ não é um conjunto de conectivos funcionalmente completo. Idem para $\{\to, \vee\}$ (sugestão: mostre que para cada fórmula $\varphi$ com apenas $\to$ e $\vee$ existe uma valoração $v$ tal que $[\![\varphi]\!]_v = 1$).

4. Mostre que a barra de Sheffer, $|$, forma um conjunto funcionalmente completo (sugestão: $\models \neg\varphi \leftrightarrow \varphi|\varphi$).

5. Mostre que o conectivo $\downarrow$ ($\varphi$ *nem* $\psi$), com função de valoração $[\![\varphi \downarrow \psi]\!] = 1$ sse $[\![\varphi]\!] = [\![\psi]\!] = 0$ forma um conjunto funcionalmente completo.

6. Mostre que $|$ e $\downarrow$ são os únicos conectivos binários \$ tais que $\{\,\$\,\}$ é funcionalmente completo.

7. A completude funcional de $\{\vee, \neg\}$ pode ser demonstrada de uma forma alternativa.
   Seja \$ um conectivo $n$-ário com função de valoração $[\![\$(p_1, \ldots, p_n)]\!] = f([\![p_1]\!], \ldots, [\![p_n]\!])$. Queremos encontrar uma proposição $\tau$ (em $\{\vee, \neg\}$) tal que $[\![\tau]\!] = f([\![p_1]\!], \ldots, [\![p_n]\!])$.

   Suponha que $f([\![p_1]\!], \ldots, [\![p_n]\!]) = 1$ ao menos uma vez. Considere todas as uplas $([\![p_1]\!], \ldots, [\![p_n]\!])$ com $f([\![p_1]\!], \ldots, [\![p_n]\!]) = 1$ e forme as conjunções correspondentes $\bar{p}_1 \wedge \bar{p}_2 \wedge \ldots \wedge \bar{p}_n$ tais que $\bar{p}_i = p_i$ se $[\![p_i]\!] = 1$, $\bar{p}_i = \neg p_i$ se $[\![p_i]\!] = 0$. Então mostre que $\models (\bar{p}_1^1 \wedge \bar{p}_2^1 \wedge \ldots \wedge \bar{p}_n^1) \vee \ldots \vee (\bar{p}_1^k \wedge \bar{p}_2^k \wedge \ldots \wedge \bar{p}_n^k) \leftrightarrow \$(p_1, \ldots, p_n)$, onde a disjunção é tomada sobre todas as $n$-uplas tais que $f([\![p_1]\!], \ldots, [\![p_n]\!]) = 1$.

   Alternativamente, podemos considerar as uplas para as quais $f([\![p_1]\!], \ldots, [\![p_n]\!]) = 0$. Preencha os detalhes. Note que esta demonstração da completude funcional prova ao mesmo tempo os Teoremas da Forma Normal.

8. Seja o conectivo ternário \$ definido por $[\![\$(\varphi_1, \varphi_2, \varphi_3)]\!] = 1 \Leftrightarrow [\![\varphi_1]\!] + [\![\varphi_2]\!] + [\![\varphi_3]\!] \geq 2$ (o conectivo 'maioria'). Exprima \$ em termos de $\vee$ e $\neg$.

9. Seja o conectivo binário # definido pela tabela

| # | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

   Exprima # em termos de $\vee$ e $\neg$.

10. Determine as formas normais conjuntivas e disjuntivas para $\neg(\varphi \leftrightarrow \psi)$, $((\varphi \to \psi) \to \psi) \to \psi$, $(\varphi \to (\varphi \wedge \neg\psi)) \wedge (\psi \to (\psi \wedge \neg\varphi))$.

11. Dê um critério para que uma forma normal conjuntiva seja uma tautologia.

12. Demonstre que $\bigwedge_{i \leq n} \varphi_i \vee \bigwedge_{j \leq m} \psi_j \approx \bigwedge_{\substack{i \leq n \\ j \leq m}} (\varphi_i \vee \psi_j)$ e

    $\bigvee_{i \leq n} \varphi_i \wedge \bigvee_{j \leq m} \psi_j \approx \bigvee_{\substack{i \leq n \\ j \leq m}} (\varphi_i \wedge \psi_j)$.

13. O conjunto de todas as valorações, visto como o conjunto de todas as seqüências 0-1, forma um espaço topológico, o chamado espaço de Cantor $\mathcal{C}$. Os conjuntos abertos básicos são uniões finitas de conjuntos da forma $\{v \mid [\![p_i]\!]_v = \ldots = [\![p_{i_n}]\!]_v = 1 \text{ e } [\![p_{j_1}]\!]_v = \ldots = [\![p_{j_m}]\!]_v = 0\}$, $i_k \neq j_p$ para $k \leq n$; $p \leq m$.

    Defina uma função $[\![\ ]\!] : PROP \to \mathcal{P}(\mathcal{C})$ (subconjuntos do espaço de Cantor) por: $[\![\varphi]\!] = \{v \mid [\![\varphi]\!]_v = 1\}$.

    (a) Mostre que $[\![\varphi]\!]$ é um conjunto aberto básico (que também é fechado),

    (b) $[\![\vee\psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!]$; $[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$; $[\![\neg\varphi]\!] = [\![\varphi]\!]^{\wedge}$,

    (c) $\models \varphi \Leftrightarrow [\![\varphi]\!] = C$; $[\![\perp]\!] = \emptyset$; $\models \varphi \to \psi \Leftrightarrow [\![\varphi]\!] \subseteq [\![\psi]\!]$.

    Estenda o mapeamento para conjuntos de proposições $\Gamma$ por $[\![\Gamma]\!] = \{v \mid [\![\varphi]\!]_v = 1 \text{ para todo } \varphi \in \Gamma\}$. Note que $[\![\Gamma]\!]$ é fechado.

    (d) $\Gamma \models \varphi \Leftrightarrow [\![\Gamma]\!] \subseteq [\![\varphi]\!]$.

14. Podemos ver a relação $\models \varphi \to \psi$ como uma espécie de ordenação. Ponha $\varphi \sqsubset \psi := \models \varphi \to \psi$ e $\not\models \psi \to \varphi$.

    (i) para cada $\varphi, \psi$ tais que $\varphi \sqsubset \psi$, encontre $\sigma$ com $\varphi \sqsubset \sigma \sqsubset \psi$,

    (ii) encontre $\varphi_1, \varphi_2, \varphi_3, \ldots$, tais que $\varphi_1 \sqsubset \varphi_2 \sqsubset \varphi_3 \sqsubset \varphi_4 \sqsubset \ldots$,

    (iii) mostre que para cada $\varphi, \psi$ com $\varphi$ e $\psi$ incomparáveis, existe pelo menos um $\sigma$ com $\varphi, \psi \sqsubset \sigma$.

15. Dê uma definição recursiva da substituição simultânea. $\varphi[\psi_1, \ldots, \psi_n/p_1, \ldots, p_n]$ e formule e demonstre o análogo apropriado do Teorema da Substituição (teorema 1.2.6).

## 1.4 Dedução Natural

Nas seções precedentes adotamos a visão de que a lógica proposicional é baseada nas tabelas-verdade, i.e. olhamos para a lógica do ponto de vista semântico. Essa, entretanto, não é a única visão possível. Se se pensa em lógica como uma codificação do raciocínio (exato), então ela deveria permanecer próxima à prática de se fazer inferência, ao invés de se basear na noção de verdade. Agora exploraremos a abordagem não-semântica, definindo um sistema para derivar conclusões a partir de premissas. Embora essa abordagem seja de natureza formal, i.e. se abstenha de interpretar os enunciados e as regras, é aconselhável manter em mente alguma interpretação. Vamos introduzir um número de regras de derivação, que são, até certo ponto, os passos atômicos em uma derivação. Essas regras de derivação são concebidas (por Gentzen), para reproduzir o significado intuitivo dos conectivos tão fielmente quanto possível.

Existe um pequeno problema, que ao mesmo tempo é uma grande vantagem, nomeadamente: nossas regras exprimem o significado construtivo dos conectivos. Essa vantagem não será explorada agora, mas é bom guardá-la na memória quando lidamos com lógica (a vantagem é explorada na lógica intuicionística).

Um exemplo simples: o princípio do terceiro excluído nos diz que $\models \varphi \vee \neg\varphi$, i.e., assumindo que $\varphi$ é um enunciado matemático definido, ou ele ou sua negação deve ser verdadeiro(a). Agora considere um determinado problema ainda não resolvido, como por exemplo a Hipótese de Riemann, chame-a $R$. Então ou $R$ é verdadeiro, ou $\neg R$ é verdadeiro. Entretanto, não sabemos qual dos dois é verdadeiro, portanto o conteúdo construtivo de $R \vee \neg R$ é nulo. Construtivamente, seria necessário um método para encontrar qual das alternativas se verifica.

O conectivo proposicional que tem um significado bem diferente em uma abordagem construtiva e em uma abordagem não-construtiva é a disjunção. Por conseguinte restringimos nossa linguagem no momento aos conectivos $\wedge$, $\rightarrow$, e $\perp$. Essa não é uma restrição real pois $\{\rightarrow, \perp\}$ é um conjunto funcionalmente completo.

Nossas derivações consistem de passos muito simples, tais como "de $\varphi$ e $\varphi \rightarrow \psi$ conclua $\psi$", escrito da seguinte forma:

$$\frac{\varphi \qquad \varphi \rightarrow \psi}{\psi}$$

As proposições acima da linha são *premissas*, e a que está abaixo da linha é a *conclusão*. O exemplo acima *eliminou* o conectivo $\rightarrow$. Podemos também *introduzir* conectivos. As regras de derivação para $\wedge$ e $\rightarrow$ são divididas em

| REGRAS DE INTRODUÇÃO | REGRAS DE ELIMINAÇÃO |
|---|---|
| $(\wedge I)\quad \dfrac{\varphi \quad \psi}{\varphi \wedge \psi}\wedge I$ | $(\wedge E)\quad \dfrac{\varphi \wedge \psi}{\varphi}\wedge E \quad \dfrac{\varphi \wedge \psi}{\psi}\wedge E$ |
| $(\rightarrow I)\quad \begin{array}{c}[\varphi]\\ \vdots \\ \dfrac{\psi}{\varphi \rightarrow \psi}\rightarrow I\end{array}$ | $(\rightarrow E)\quad \dfrac{\varphi \qquad \varphi \rightarrow \psi}{\psi}\rightarrow E$ |

Temos duas regras para $\perp$, ambas eliminam $\perp$, mas introduzem uma fórmula.

$$(\perp)\quad \frac{\perp}{\varphi}\,\perp \qquad\qquad (\mathrm{RAA})\quad \frac{\begin{matrix}[\neg\varphi]\\ \vdots\\ \perp\end{matrix}}{\varphi}\,\mathrm{RAA}$$

Como de costume '$\neg\varphi$' é usada aqui como uma abreviação para '$\varphi \to \perp$'.

As regras para $\wedge$ são evidentes: se temos $\varphi$ e $\psi$ podemos concluir $\varphi \wedge \psi$, e se temos $\varphi \wedge \psi$ podemos concluir $\varphi$ (ou $\psi$). A regra de introdução para a implicação tem uma forma diferente. Ela enuncia que, se podemos derivar $\psi$ a partir de $\varphi$ (como uma hipótese), então podemos concluir $\varphi \to \psi$ (sem a hipótese $\varphi$). Isso está de acordo com o significado intuitivo da implicação: $\varphi \to \psi$ significa que "$\psi$ segue de $\varphi$". Escrevemos a regra $(\to I)$ na forma acima para sugerir uma derivação. A notação ficará mais clara depois que tivermos definido derivações. Por enquanto escreveremos as premissas de uma regra na ordem que parece mais apropriada, e mais tarde seremos mais exigentes.

A regra $(\to E)$ também é evidente considerando o significado da implicação. Se $\varphi$ é dado e sabemos que $\psi$ segue de $\varphi$, então temos também $\psi$. A *regra do falsum*, $(\perp)$, expressa que a partir de um absurdo podemos derivar qualquer coisa (em latim *ex falso sequitur quodlibet*), e a *regra de reductio ad absurdum*, (RAA), é uma formulação do *princípio da prova por contradição*: se se deriva uma contradição a partir da hipótese $\neg\varphi$, então tem-se uma derivação de $\varphi$ (sem a hipótese $\neg\varphi$, é claro). Em ambos $(\to I)$ e (RAA) as hipóteses desaparecem, e isso é indicado por um traço riscando a hipótese. Dizemos que a hipótese é *cancelada*. Vamos abrir um parênteses aqui e falar um pouco sobre o cancelamento de hipóteses. Primeiramente consideremos a introdução da implicação. Existe um teorema bem conhecido em geometria plana que enuncia "se um triângulo é isósceles, então os ângulos opostos aos lados iguais são iguais entre si" (*Elementos*, de Euclides, Livro I, proposição 5). Isso é demonstrado da seguinte maneira: supomos que temos um triângulo isósceles e então, em um certo número de passos, deduzimos que os ângulos na base são iguais. Daí concluímos que *os ângulos na base são iguais se o triângulo é isósceles*.

Pergunta 1: ainda precisamos da hipótese de que o triângulo é isósceles? É claro que não! Incorporamos, por assim dizer, essa condição no enunciado propriamente dito. É precisamente o papel dos enunciados condicionais, tais como "se chover usarei meu guarda-chuva", para se livrar da obrigação de requerer (ou verificar) a condição. Em resumo: se podemos deduzir $\psi$ usando a hipótese $\varphi$, então $\varphi \to \psi$ é o caso *sem a hipótese* $\varphi$ (pode haver outras hipóteses, obviamente).

Pergunta 2: é proibido manter a hipótese? Resposta: não, mas ela é claramente supérflua. Na verdade em geral sentimos que as condições supérfluas são confusas ou até mesmo enganosas, mas isso é muito mais uma questão da psicologia da resolução de problemas do que de lógica formal. Normalmente queremos o melhor resultado possível, e é intuitivamente claro que quanto mais hipóteses enunciamos para um teorema, mais fraco é o nosso resultado. Por conseguinte cancelaremos, via de regra, tantas hipóteses quanto possível.

No caso do reductio ad absurdum também temos que lidar com o cancelamento de hipóteses. Novamente, vamos considerar um exemplo.

Em Análise introduzimos a noção de *seqüência convergente* $(a_n)$ e posteriormente a noção "$a$ é um limite de $(a_n)$". O próximo passo é demonstrar que para cada seqüência convergente existe um único limite; estamos interessados na parte da demonstração que mostra que existe no máximo um limite. Tal demonstração pode se processar da seguinte maneira: assumimos que existem dois limites distintos $a$ e $a'$, e a partir dessa hipótese, $a \neq a'$, derivamos uma contradição. Conclusão: $a = a'$. Nesse caso desprezamos a hipótese $a \neq a'$, dessa vez não é o caso de ser supérflua, mas de estar em conflito! Logo, tanto no caso de $(\to I)$ quanto no de (RAA), é prática segura cancelar todas as ocorrências da hipótese em aberto.

Para dominar a técnica da Dedução Natural, e para se familiarizar com a técnica de cancelamento de hipóteses, nada melhor que olhar para alguns casos concretos. Portanto, antes de proceder à noção de *derivação*, consideremos alguns exemplos.

$$\textbf{I} \quad \dfrac{\dfrac{\dfrac{[\varphi \wedge \psi]^1}{\psi}\wedge E \qquad \dfrac{[\varphi \wedge \psi]^1}{\varphi}\wedge E}{\psi \wedge \varphi}\wedge I}{\varphi \wedge \psi \to \psi \wedge \varphi}\to I_1 \qquad\qquad \textbf{II} \quad \dfrac{\dfrac{\dfrac{[\varphi]^2 \quad [\varphi \to \bot]^1}{\bot}\to E}{(\varphi \to \bot) \to \bot}\to I_1}{\varphi \to ((\varphi \to \bot) \to \bot)}\to I_2$$

$$\textbf{III} \quad \dfrac{\dfrac{\dfrac{\dfrac{[\varphi \wedge \psi]^1}{\psi}\wedge E \qquad \dfrac{\dfrac{[\varphi \wedge \psi]^1}{\varphi}\wedge E \qquad [\varphi \to (\psi \to \sigma)]^2}{\psi \to \sigma}\to E}{\sigma}\to E}{\varphi \wedge \psi \to \sigma}\to I_1}{(\varphi \to (\psi \to \sigma)) \to (\varphi \wedge \psi \to \sigma)}\to I_2$$

Se usarmos a abreviação usual '$\neg\varphi$' para '$\varphi \to \bot$', podemos trazer algumas derivações para uma forma mais conveniente. (Recordemos que $\neg\varphi$ e $\varphi \to \bot$, como foram dados em 1.2, são semanticamente equivalentes). Reescrevemos a derivação **II** usando a abreviação:

$$\textbf{II}' \quad \dfrac{\dfrac{\dfrac{[\varphi]^2 \quad [\neg\varphi]^1}{\bot}\to E}{\neg\neg\varphi}\to I_1}{\varphi \to \neg\neg\varphi}\to I_2$$

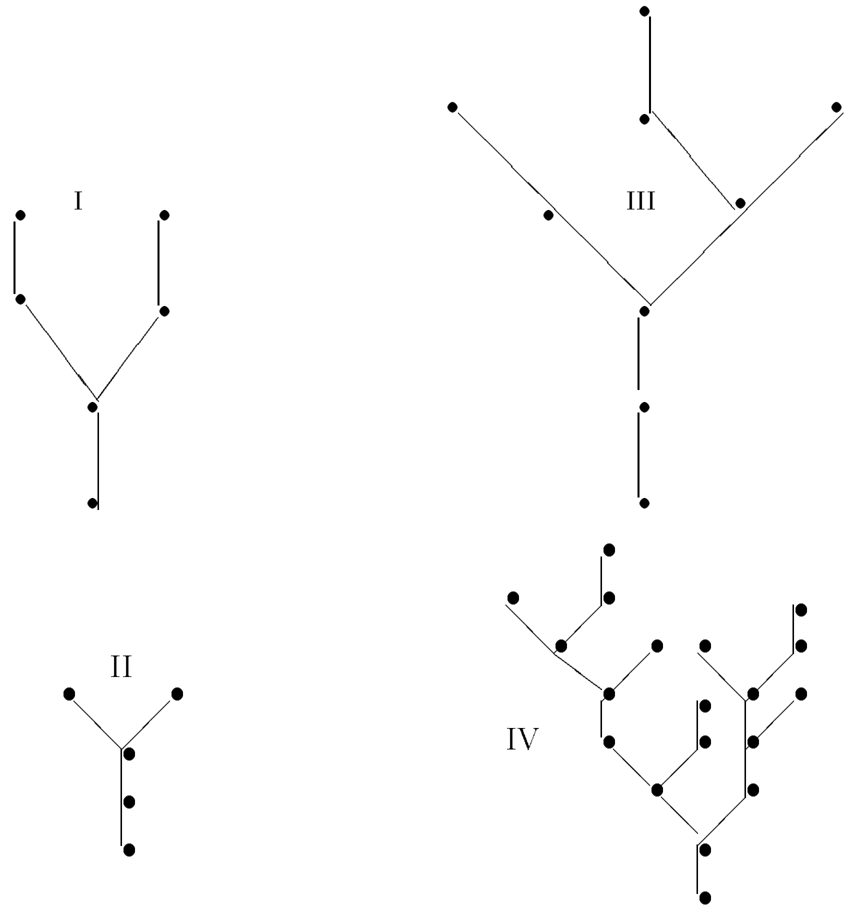
No exemplo seguinte usamos o símbolo de negação e também o de bi-implicação;

$\varphi \leftrightarrow \psi$ para $(\varphi \to \psi) \wedge (\psi \to \varphi)$.

**IV**

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{
          [\varphi]^1 \quad \dfrac{[\varphi \leftrightarrow \neg\varphi]^3}{\varphi \to \neg\varphi}\,\wedge E
        }{\neg\varphi}\,{\to}E
        \quad [\varphi]^1
      }{\perp}\,{\to}E
    }{\neg\varphi}\,{\to}I_1
    \quad
    \dfrac{[\varphi \leftrightarrow \neg\varphi]^3}{\neg\varphi \to \varphi}\,\wedge E
  }{\varphi}\,{\to}E
  \quad
  \dfrac{
    \dfrac{
      \dfrac{
        [\varphi]^2 \quad \dfrac{[\varphi \leftrightarrow \neg\varphi]^3}{\varphi \to \neg\varphi}\,\wedge E
      }{\neg\varphi}\,{\to}E
      \quad [\varphi]^2
    }{\perp}\,{\to}E
  }{\neg\varphi}\,{\to}I_2
}{
  \dfrac{\perp}{\neg(\varphi \leftrightarrow \neg\varphi)}\,{\to}I_3
}\,{\to}E
$$

Os exemplos nos mostram que derivações têm a forma de árvores. Mostramos as árvores abaixo:




Pode-se também apresentar derivações como cadeias (lineares) de proposições: permaneceremos, entretanto com a forma de árvore, e a idéia é que aquilo que vem naturalmente na forma de árvore não deveria ser colocado numa cadeia.

Agora temos que definir a noção de *derivação* em geral. Usaremos uma definição indutiva para produzir árvores.

*Notação.* se $\begin{matrix}\mathcal{D}\\ \varphi\end{matrix}$, $\begin{matrix}\mathcal{D}'\\ \varphi'\end{matrix}$ são derivações com conclusões $\varphi, \varphi'$, então $\dfrac{\begin{matrix}\mathcal{D}\\ \varphi\end{matrix}}{\psi}$, $\dfrac{\begin{matrix}\mathcal{D}\\ \varphi\end{matrix} \quad \begin{matrix}\mathcal{D}'\\ \varphi'\end{matrix}}{\psi}$ são derivações obtidas aplicando-se uma regra de derivação a $\varphi$ (e a $\varphi$ e $\varphi'$). O cancelamento de uma hipótese é indicado da seguinte maneira: se $\begin{matrix}\mathcal{D}\\ \varphi\end{matrix}$ é uma derivação com hipótese $\psi$, então $\dfrac{\begin{matrix}[\varphi]\\ \mathcal{D}\\ \varphi\end{matrix}}{\sigma}$ é uma derivação com $\psi$ cancelada.

Com respeito ao cancelamento de hipóteses, observamos que não se cancela necessariamente *todas* as ocorrências de uma tal proposição $\psi$. Isso é claramente justificado, pois nota-se que ao adicionar hipóteses não se faz com que uma proposição seja inderivável (informação irrelevante pode sempre ser adicionada). É uma questão de prudência, entretanto, cancelar tanto quanto possível. Por que prosseguir com mais hipóteses do que o necessário?

Além do mais, pode-se aplicar $(\to I)$ se não há hipótese disponível para o cancelamento e.g. $\dfrac{\varphi}{\psi \to \varphi} \to I$ é uma derivação correta, usando apenas $(\to I)$. Para resumir: dada uma árvore de derivação de $\psi$, obtemos uma árvore de derivação de $\varphi \to \psi$ (ou $\psi$) no fundo da árvore e cancelando algumas (ou todas) as ocorrências, e cancelando algumas (ou todas) as ocorrências, se existe alguma, de $\varphi$ (ou $\neg\varphi$) localizada no alto da árvore.

Algumas palavras sobre o uso prático da dedução natural: se você deseja construir uma derivação para uma proposição é aconselhável conceber algum tipo de estratégia, tal qual num jogo. Suponha que você quer mostrar que $(\varphi \to (\psi \to \sigma)) \to (\varphi \wedge \psi \to \sigma)$ (Exemplo **III**), então (como a proposição é uma fórmula implicacional) a regra $(\to I)$ sugere a si própria. Portanto tente derivar $\varphi \wedge \psi\sigma$ a partir da hipótese $\varphi \to (\psi \to \sigma)$. Agora sabemos onde começar e para onde ir. Para usar $\varphi \to (\psi \to \sigma)$ desejamos ter $\varphi$ (para aplicar $(\to E)$). Por outro lado desejamos derivar $\sigma$ a partir de $\varphi \wedge \psi$, logo podemos usar $\varphi \wedge \psi$ como uma hipótese. Mas disso podemos imediatamente obter $\varphi$. Agora uma aplicação de $(\to E)$ resulta em $\psi \to \sigma$. Novamente precisamos de algo para "quebrar $\psi \to \sigma$ em suas partes menores"; isso é claramente $\psi$. Mas $\psi$ é fornecido pela hipótese $\varphi \wedge \psi$. Como resultado, obtivemos $\sigma$ – tal qual desejávamos. Agora algumas regras de introdução produzião o resultado desejado. A derivação **III** mostra em detalhe como construir a derivação resultante. Depois de se construir um certo número de derivações adquire-se a convicção prática de que se deve primeiramente quebrar as proposições em suas partes menores na direção debaixo-para-cima, e então constrói-se as proposições desejadas juntando-se as partes resultantes de maneira apropriada. Essa convicção prática é confirmada pelo *Teorema da Normalização*, para o qual retornaremos mais adiante. Há um ponto que tende particularmente a confundir principiantes:

$$\dfrac{\begin{matrix}[\varphi]\\ \vdots\\ \bot\end{matrix}}{\neg\varphi} \to I \qquad \text{e} \qquad \dfrac{\begin{matrix}[\neg\varphi]\\ \vdots\\ \bot\end{matrix}}{\varphi}\,\text{RAA}$$

se parecem muito. São ambas casos particulares de Reductio ad absurdum? Na verdade a derivação à esquerda nos diz (informalmente) que a suposição de $\varphi$ leva a uma contradição, logo $\varphi$ *não pode ser o caso*. Isso é em nossa terminologia o significado de "não $\varphi$". A derivação à direita nos diz que a suposição de $\neg\varphi$ leva a uma contradição, portanto (pelo mesmo raciocínio) $\neg\varphi$ não pode ser o caso. Logo, pelo significado da negação, obteríamos apenas $\neg\neg\varphi$. Não está de forma alguma claro que $\neg\neg\varphi$ é equivalente a $\varphi$ (de fato, isso é rejeitado pelos intuicionistas), logo essa é uma propriedade extra de nossa lógica. (Isso é confirmado num sentido técnico: $\neg\neg\varphi \to \varphi$ não é derivável no sistema sem RAA.)

Retornamos agora às noções teóricas.

**Definição 1.4.1** O conjunto de derivações é o menor conjunto $X$ tal que

(1) A árvore de um único elemento $\varphi$ pertence a $X$ para toda $\varphi \in PROP$.

(2$\wedge$) Se $\begin{array}{c}\mathcal{D}\\ \varphi\end{array}, \begin{array}{c}\mathcal{D}'\\ \varphi'\end{array} \in X$ então $\dfrac{\begin{array}{cc}\mathcal{D} & \mathcal{D}'\\ \varphi & \varphi'\end{array}}{\varphi \wedge \varphi'} \in X$.

Se $\begin{array}{c}\mathcal{D}\\ \varphi \wedge \psi\end{array} \in X$, então $\dfrac{\begin{array}{c}\mathcal{D}\\ \varphi \wedge \psi\end{array}}{\varphi}, \dfrac{\begin{array}{c}\mathcal{D}\\ \varphi \wedge \psi\end{array}}{\psi} \in X$.

(2$\to$) Se $\begin{array}{c}\varphi\\ \mathcal{D}\\ \psi\end{array} \in X$, então $\dfrac{\begin{array}{c}[\varphi]\\ \mathcal{D}\\ \psi\end{array}}{\varphi \to \psi} \in X$.

Se $\begin{array}{c}\mathcal{D}\\ \varphi\end{array}, \begin{array}{c}\mathcal{D}'\\ \varphi \to \psi\end{array} \in X$ então $\dfrac{\begin{array}{cc}\mathcal{D} & \mathcal{D}'\\ \varphi & \varphi \to \psi\end{array}}{\psi} \in X$.

(2$\perp$) Se $\begin{array}{c}\mathcal{D}\\ \perp\end{array} \in X$, então $\dfrac{\begin{array}{c}\mathcal{D}\\ \perp\end{array}}{\varphi} \in X$.

Se $\begin{array}{c}\neg\varphi\\ \mathcal{D}\\ \perp\end{array} \in X$, então $\dfrac{\begin{array}{c}[\neg\varphi]\\ \mathcal{D}\\ \perp\end{array}}{\varphi} \in X$.

A fórmula no final de uma derivação é chamada de *conclusão* da derivação. Como a classe das derivações é indutivamente definida, podemos reproduzir os resultados da seção 1.1.

E.g. temos um *princípio da indução sobre* $\mathcal{D}$: seja $A$ uma propriedade. Se $A(\mathcal{D})$ se verifica para derivações com apenas um elemento e $A$ é preservada sob as cláusulas (2$\wedge$), (2 $\to$) e (2$\perp$), então $A(\mathcal{D})$ se verifica para todas as derivações. Igualmente podemos definir funções sobre o conjunto de derivações por recursão (cf. Exercício 6, 7, 9).

**Definição 1.4.2** A relação $\Gamma \vdash \varphi$ entre conjuntos de proposições e proposições é definida por: existe uma derivação com conclusão $\varphi$ e com todas as hipóteses (não canceladas) em $\Gamma$. (Veja também o Exercício 6).

Dizemos que $\varphi$ é *derivável* a partir de $\Gamma$. Note que pela definição $\Gamma$ pode conter várias "hipóteses" supérfluas. O símbolo $\vdash$ é chamado de *roleta*.

Se $\Gamma =$, escrevemos $\vdash \varphi$, e dizemos que $\varphi$ é um teorema.

Poderíamos ter evitado a noção de 'derivação' e ao invés dela ter tomado a noção de 'derivabilidade' como fundamental, veja Exercício 10. As duas noções, entretanto, são intimamente relacionadas.

**Lema 1.4.3**
(a) $\Gamma \vdash \varphi$ *se* $\varphi \in \Gamma$,
(b) $\Gamma \vdash \varphi,\ \Gamma' \vdash \psi \Rightarrow \Gamma \cup \Gamma' \vdash \varphi \wedge \psi$,
(c) $\Gamma \vdash \varphi \wedge \psi \Rightarrow \Gamma \vdash \varphi$ *e* $\Gamma \vdash \psi$,
(d) $\Gamma \cup \varphi \vdash \psi \Rightarrow \Gamma \vdash \varphi \to \psi$,
(e) $\Gamma \vdash \varphi,\ \Gamma' \vdash \varphi \to \psi \Rightarrow \Gamma \cup \Gamma' \vdash \psi$,
(f) $\Gamma \vdash \perp \Rightarrow \Gamma \vdash \varphi$,
(g) $\Gamma \cup \{\neg\varphi\} \vdash \perp \Rightarrow \Gamma \vdash \varphi$.

*Demonstração.* Imediata a partir da definição de derivação. □

Agora vamos listar alguns teoremas. $\neg$ e $\leftrightarrow$ são usados como abreviações.

**Teorema 1.4.4**
(1) $\vdash \varphi \to (\psi \to \varphi)$,
(2) $\vdash \varphi \to (\neg\varphi \to \psi)$,
(3) $\vdash (\varphi \to \psi) \to ((\psi \to \sigma) \to (\varphi \to \sigma))$,
(4) $\vdash (\varphi \to \psi) \leftrightarrow (\neg\psi \to \neg\varphi)$,
(5) $\vdash \neg\neg\varphi \leftrightarrow \varphi$,
(6) $\vdash (\varphi \to (\psi \to \sigma)) \leftrightarrow (\varphi \wedge \psi \to \sigma)$,
(7) $\vdash \perp \leftrightarrow (\varphi \wedge \neg\varphi)$.

*Demonstração.*

1. $$\dfrac{\dfrac{[\varphi]^1}{\psi \to \varphi}\to I}{\varphi \to (\psi \to \varphi)}\to I_1$$

2. $$\dfrac{\dfrac{\dfrac{\dfrac{[\varphi]^2 \quad [\neg\varphi]^1}{\perp}\to E}{\psi}\perp}{\neg\varphi \to \psi}\to I_1}{\varphi \to (\neg\varphi \to \psi)}\to I_2$$

3. $$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\varphi]^1 \quad [\varphi \to \psi]^3}{\psi}\to E \qquad [\psi \to \sigma]^2}{\sigma}\to E}{\varphi \to \sigma}\to I_1}{(\psi \to \sigma) \to (\varphi \to \sigma)}\to I_2}{(\varphi \to \psi) \to ((\psi \to \sigma) \to (\varphi \to \sigma))}\to I_3$$

4. Para uma direção, substitua $\sigma$ por $\perp$ em 3, então $\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$.

Reciprocamente:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\neg\psi]^1 \quad [\neg\psi \to \neg\varphi]^3}{\neg\varphi} \to E \qquad [\varphi]^2}{\perp} \to E}{\psi} \text{RAA}_1}{\varphi \to \psi} \to I_2}{(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)} \to I_3$$

Portanto agora temos $\dfrac{\begin{matrix} \mathcal{D} & & \mathcal{D}' \\ (\varphi \to \psi) \to (\neg\psi \to \neg\varphi) & & (\neg\psi \to \neg\varphi) \to (\varphi \to \psi) \end{matrix}}{(\varphi \to \psi) \leftrightarrow (\neg\psi \to \neg\varphi)}$

5. Já demonstramos $\varphi \to \neg\neg\varphi$ como um exemplo. Reciprocamente:

$$\dfrac{\dfrac{\dfrac{[\neg\varphi]^1 \quad [\neg\neg\varphi]^2}{\perp} \to E}{\varphi} \text{RAA}_1}{\neg\neg\varphi \to \varphi} \to I_2$$

O resultado agora segue imediatamente. Os números 6 e 7 são deixados para o leitor. □

O sistema delineado nesta seção é chamado de "cálculo de dedução natural" por uma boa razão. Isto é: sua forma de fazer inferências corresponde ao raciocínio que usamos intuitivamente. As regras apresentam meios pelos quais se pode quebrar fórmulas, ou juntá-las. Uma derivação então consiste de uma manipulação habilidosa das regras, cujo uso é usualmente sugerido pela forma da fórmula que desejamos provar.

Discutiremos um exemplo de modo a ilustrar a estratégia geral de construção de derivações. Vamos considerar a recíproca do nosso exemplo anterior **III**.

Para provar $(\varphi \wedge \psi \to \sigma) \to (\varphi \to (\psi \to \sigma))$ existe apenas um único passo inicial: supor $\varphi \wedge \psi \to \sigma$ e tentar derivar $\varphi \to (\psi \to \sigma)$. Agora podemos olhar para a suposição ou para o resultado desejado. Vamos considerar a última opção inicialmente: para provar $\varphi \to (\psi \to \sigma)$, devemos supor $\varphi$ e derivar $\psi \to \sigma$, mas para esse último caso devemos supor $\psi$ e derivar $\sigma$.

Logo, podemos supor ao mesmo tempo $\varphi \wedge \psi \to \sigma$, $\varphi$ e $\psi$. Agora o procedimento sugere a si próprio: derive $\varphi \wedge \psi$ a partir de $\varphi$ e $\psi$, e $\sigma$ a partir de $\varphi \wedge \psi$ e $\varphi \wedge \psi \to \sigma$.

Colocando tudo junto, obtemos a seguinte derivação:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\varphi]^2 \quad [\psi]^1}{\varphi \wedge \psi} \wedge I \qquad [\varphi \wedge \psi \to \sigma]^3}{\sigma} \to E}{\psi \to \sigma} \to I_1}{\varphi \to (\psi \to \sigma)} \to I_2}{(\varphi \wedge \psi \to \sigma) \to (\varphi \to (\psi \to \sigma))} \to I_3$$

Se tivéssemos considerado primeiro $\varphi \wedge \psi \to \sigma$, então a única maneira de seguir adiante seria adicionar $\varphi \wedge \psi$ e aplicar $\to E$. Agora $\varphi \wedge \psi$ ou permanece como uma suposição, ou é obtida a partir de uma outra coisa. Imediatamente ocorre ao leitor derivar $\varphi \wedge \psi$ a partir de $\varphi$ e $\psi$. Mas agora ele terá que construir a derivação que obtivemos acima.

Por mais simples que esse exemplo pareça, existem complicações. Em particular a regra de reductio ad absurdum não é nem de perto tão natural quanto as outras regras. Seu uso tem que ser aprendido praticando-se; além disso uma certa habilidade para perceber a distinção entre o *construtivo* e o *não-construtivo* será útil quando se vai tentar decidir quando usá-la.

Finalmente, recordamos que $\top$ é uma abreviação de $\neg\bot$ (i.e. $\bot \to \bot$).

**Exercícios**

1. Demonstre que as seguintes proposições são deriváveis.

$$\begin{array}{llll} (a) & \varphi \to \varphi, & (d) & (\varphi \to \psi) \leftrightarrow \neg(\varphi \wedge \neg\psi), \\ (b) & \bot \to \varphi, & (e) & (\varphi \wedge \psi) \leftrightarrow \neg(\varphi \to \neg\psi), \\ (c) & \neg(\varphi \wedge \neg\varphi), & (f) & \varphi \to (\psi \to \varphi \wedge \psi). \end{array}$$

2. Idem para

$$\begin{array}{ll} (a) & (\varphi \to \neg\varphi) \to \neg\varphi, \\ (b) & (\varphi \to (\psi \to \sigma)) \leftrightarrow (\psi \to (\varphi \to \sigma)), \\ (c) & (\varphi \to \psi) \wedge (\varphi \to \neg\psi) \to \neg\varphi, \\ (d) & (\varphi \to \psi) \to ((\varphi \to (\psi \to \sigma)) \to (\varphi \to \sigma)). \end{array}$$

3. Demonstre que

$$\begin{array}{llll} (a) & \varphi \vdash \neg(\neg\varphi \wedge \psi), & (d) & \vdash \varphi \Rightarrow \vdash \psi \to \varphi, \\ (b) & \neg(\varphi \wedge \neg\psi), \varphi \vdash \psi, & (e) & \neg\varphi \vdash \varphi \to \psi. \\ (c) & \neg\varphi \vdash (\varphi \to \psi) \leftrightarrow \neg\varphi, & & \end{array}$$

4. Demonstre que $\vdash ((\varphi \to \psi) \to (\varphi \to \sigma)) \to ((\varphi \to (\psi \to \sigma)))$,
$\vdash ((\varphi \to \psi) \to \varphi) \to \varphi)$.

5. Demonstre que $\Gamma \vdash \varphi \Rightarrow \Gamma \cup \Delta \vdash \varphi$,
$\Gamma \vdash \varphi; \Delta, \varphi \vdash \psi \Rightarrow \Gamma \cup \Delta \vdash \psi$.

6. Dê uma definição recursiva da função $Hyp$ que associa a cada derivação $\mathcal{D}$ seu conjunto de hipóteses $Hyp(\mathcal{D})$ (trata-se de uma noção mais estrita que a noção apresentada na definição 1.4.2, pois esta refere-se ao menor conjunto de hipóteses, i.e. hipóteses sem 'lixo').

7. Análogo ao operador de substituição para proposições definimos um operador de substituição para derivações. $\mathcal{D}[\varphi/p]$ é obtida substituindo-se cada ocorrência de $p$ em cada proposição em $\mathcal{D}$ por $\varphi$. Dê uma definição recursiva de $\mathcal{D}[\varphi/p]$. Demonstre que $\mathcal{D}[\varphi/p]$ é uma derivação se $\mathcal{D}$ é uma derivação, e que $\Gamma \vdash \sigma \Rightarrow \Gamma[\varphi/p] \vdash \sigma[\varphi/p]$. Observação: em muitos casos se necessita de noções mais refinadas de substituição, mas esta nos será suficiente.

8. **(Teorema da Substituição)** $\vdash (\varphi_1 \leftrightarrow \varphi_2) \to (\psi[\varphi_1/p] \leftrightarrow \psi[\varphi_2/p])$.

   Sugestão: use indução sobre $\psi$; o teorema também seguirá como conseqüência do Teorema da Substituição para $\models$, uma vez que tenhamos estabelecido o Teorema da Completude.

9. O *tamanho*, $t(\mathcal{D})$, de uma derivação é o número de ocorrências de proposições em $\mathcal{D}$. Dê uma definição indutiva de $t(\mathcal{D})$. Demonstre que se pode provar propriedades de derivações por indução sobre o seu tamanho.

10. Dê uma definição recursiva da relação $\vdash$ (use a lista do Lema 1.4.3), demonstre que essa relação coincide com a relação derivada da Definição 1.4.2. Conclua que cada $\Gamma$ com $\Gamma \vdash \varphi$ contém um $\Delta$ finito, tal que $\Delta \vdash \varphi$ também.

11. Demonstre que

    $(a)$ $\vdash \top$,
    $(b)$ $\vdash \varphi \Leftrightarrow \vdash \varphi \leftrightarrow \top$,
    $(c)$ $\vdash \neg\varphi \Leftrightarrow \vdash \varphi \leftrightarrow \bot$.

## 1.5 Completude

Nesta seção demonstraremos que "veracidade" e "derivabilidade" coincidem, mais precisamente: as relações "$\models$" e "$\vdash$" coincidem. A parte fácil da alegação é: "derivabilidade" implica em "veracidade"; pois derivabilidade é estabelecida pela existência de uma derivação. Essa última noção é definida indutivamente, portanto podemos demonstrar a implicação por indução sobre a derivação.

**Lema 1.5.1 (Corretude)** *$\Gamma \vdash \varphi \Rightarrow \Gamma \models \varphi$.*

*Demonstração.* Como, pela definição 1.4.2, $\Gamma \vdash \varphi$ sse existe uma derivação $\mathcal{D}$ com todas as hipóteses em $\Gamma$, é suficiente mostrar que: para cada derivação $\mathcal{D}$ com conclusão $\varphi$ e hipóteses em $\Gamma$ temos $\Gamma \models \varphi$. Agora usamos indução sobre $\mathcal{D}$.

(*caso base*) Se $\mathcal{D}$ tem um elemento, então evidentemente $\varphi \in \Gamma$. O leitor facilmente vê que $\Gamma \models \varphi$.

$(\wedge I)$ Hipótese da indução: $\begin{array}{c}\mathcal{D}\\ \varphi\end{array}$ e $\begin{array}{c}\mathcal{D}'\\ \varphi'\end{array}$ são derivações e para cada $\Gamma$, $\Gamma'$ contendo as hipóteses de $\mathcal{D}$, $\mathcal{D}'$, $\Gamma \models \varphi$, $\Gamma' \models \varphi'$.

Agora suponha que $\Gamma''$ contém as hipóteses de $\dfrac{\begin{array}{cc}\mathcal{D} & \mathcal{D}'\\ \varphi & \varphi'\end{array}}{\varphi \wedge \varphi'}$

Escolhendo $\Gamma$ e $\Gamma'$ de tal forma que sejam exatamente o conjunto de hipóteses de $\mathcal{D}$, $\mathcal{D}'$, vemos que $\Gamma'' \supseteq \Gamma \cup \Gamma'$.

Logo $\Gamma'' \models \varphi$ e $\Gamma'' \models \varphi'$. Seja $[\![\psi]\!]_v = 1$ para toda $\psi \in \Gamma''$, então $[\![\varphi]\!]_v = [\![\varphi']\!]_v = 1$, portanto $[\![\varphi \wedge \varphi']\!]_v = 1$. Isso mostra que $\Gamma'' \models \varphi \wedge \varphi'$.

($\wedge E$) Hipótese da indução: para qualquer $\Gamma$ contendo as hipóteses de $\begin{array}{c}\mathcal{D}\\ \varphi \wedge \psi\end{array}$ temos $\Gamma \models \varphi \wedge \psi$. Considere um $\Gamma$ contendo todas as hipóteses de $\dfrac{\begin{array}{c}\mathcal{D}\\ \varphi \wedge \psi\end{array}}{\varphi}$ e $\dfrac{\begin{array}{c}\mathcal{D}\\ \varphi \wedge \psi\end{array}}{\psi}$. Deixo ao leitor a demonstração de que $\Gamma \models \varphi$ e $\Gamma \models \psi$.

($\rightarrow I$) Hipótese da indução: para qualquer $\Gamma$ contendo todas as hipóteses de $\begin{array}{c}\varphi\\ \mathcal{D}\\ \psi\end{array}$, $\Gamma \models \psi$. Suponha que $\Gamma'$ contém todas as hipóteses de $\dfrac{\begin{array}{c}[\varphi]\\ \mathcal{D}\\ \psi\end{array}}{\varphi \rightarrow \psi}$. Agora $\Gamma' \cup \{\varphi\}$ contém todas as hipóteses de $\begin{array}{c}\varphi\\ \mathcal{D}\\ \psi\end{array}$, logo se $[\![\varphi]\!] = 1$ e $[\![\chi]\!] = 1$ para toda $\chi$ em $\Gamma'$, então $[\![\psi]\!] = 1$. Portanto a tabela-verdade de $\rightarrow$ nos diz que $[\![\varphi \rightarrow \psi]\!] = 1$ se todas as proposições em $\Gamma'$ têm valor 1. Logo $\Gamma' \models \varphi \rightarrow \psi$.

($\rightarrow E$) Um exercício para o leitor.

($\perp$) Hipótese da indução: para cada $\Gamma$ contendo todas as hipóteses de $\begin{array}{c}\mathcal{D}\\ \perp\end{array}$, $\Gamma \models \perp$. Como $[\![\perp]\!] = 0$ para todas as valorações, não existe valoração tal que $[\![\psi]\!] = 1$ para toda $\psi \in \Gamma$. Suponha que $\Gamma'$ contém todas as hipóteses de $\dfrac{\begin{array}{c}\mathcal{D}\\ \perp\end{array}}{\varphi}$ e suponha que $\Gamma' \not\models \varphi$, então $[\![\psi]\!] = 1$ para toda $\psi \in \Gamma'$ e $[\![\varphi]\!] = 0$ para alguma valoração. Como $\Gamma'$ contém todas as hipóteses da primeira derivação temos uma contradição.

(RAA) Hipótese da indução: para cada $\Gamma$ contendo todas as hipóteses de $\begin{array}{c}\neg\varphi\\ \mathcal{D}\\ \perp\end{array}$, temos $\Gamma \models \perp$. Suponha que $\Gamma'$ contém todas as hipóteses de $\dfrac{\begin{array}{c}[\neg\varphi]\\ \mathcal{D}\\ \perp\end{array}}{\varphi}$ e suponha que $\Gamma' \not\models \varphi$, então existe uma valoração tal que $[\![\psi]\!] = 1$ para toda $\psi \in \Gamma'$ e $[\![\varphi]\!] = 0$, i.e. $[\![\neg\varphi]\!] = 1$. Mas $\Gamma'' = \Gamma' \cup \{\neg\varphi\}$ contém todas as hipóteses da primeira derivação e $[\![\psi]\!] = 1$ para toda $\psi \in \Gamma''$. Isto é impossível pois $\Gamma'' \models \perp$. Logo $\Gamma' \models \varphi$. □

Esse lema pode não parecer impressionante, mas ele nos permite mostrar que algumas proposições não são teoremas, através simplesmente de uma demonstração de que elas não são tautologias. Sem esse lema isso teria sido uma tarefa muito trabalhosa. Teríamos que mostrar que não existe derivação (sem hipóteses) da proposição dada. Em geral isso requer profunda percepção sobre a natureza das derivações, o que está além das nossas possibilidades no momento.

*Exemplos.* $\nvdash p_0, \nvdash (\varphi \to \psi) \to \varphi \wedge \psi$.

No primeiro exemplo, tome a valoração constante 0. $[\![p_0]\!] = 0$, logo $\not\models p_0$ e portanto $\nvdash p_0$. No segundo exemplo nos deparamos com uma meta-proposição (um *esquema*); estritamente falando ela não pode ser derivável (apenas proposições *reais* podem). Por $\vdash (\varphi \to \psi) \to \varphi \wedge \psi$ queremos dizer que todas as proposições daquela forma (obtidas substituindo-se $\varphi$ e $\psi$ por proposições reais, por exemplo) são deriváveis. Para refutá-la precisamos apenas de uma instância que não é derivável. Tome $\varphi = \psi = p_0$. Para demonstrar a recíproca do enunciado do Lema 1.5.1 precisamos de algumas novas noções. A primeira tem uma história impressionante; trata-se da noção de *ausência de contradição* ou *consistência*. Foi transformada na pedra angular dos fundamentos da matemática por Hilbert.

**Definição 1.5.2** Um conjunto $\Gamma$ de proposições é *consistente* se $\Gamma \nvdash \perp$.

Em palavras: não se pode derivar uma contradição a partir de $\Gamma$. A consistência de $\Gamma$ pode ser expressa de várias outras formas:

**Lema 1.5.3** *As seguintes condições são equivalentes:*

(i) $\Gamma$ *é consistente,*

(ii) *Para nenhuma* $\varphi$, $\Gamma \vdash \varphi$ *e* $\Gamma \vdash \neg\varphi$,

(iii) *Existe pelo menos uma* $\varphi$ *tal que* $\Gamma \nvdash \varphi$.

*Demonstração.* Vamos chamar $\Gamma$ de *inconsistente* se $\Gamma \vdash \perp$, então podemos também provar a equivalência de

(iv) $\Gamma$ é inconsistente,

(v) Existe uma $\varphi$ tal que $\Gamma \vdash \varphi$ e $\Gamma \vdash \neg\varphi$,

(vi) $\Gamma \vdash \varphi$ para toda $\varphi$.

(iv) $\Rightarrow$ (vi) Suponha que $\Gamma \vdash \perp$, i.e. existe uma derivação $\mathcal{D}$ com conclusão $\perp$ e hipóteses em $\Gamma$. Pela regra $(\perp)$ podemos adicionar uma inferência, $\perp \vdash \varphi$, a $\mathcal{D}$, de tal forma que $\Gamma \vdash \varphi$. Isso se verifica para todo $\varphi$.

(vi) $\Rightarrow$ (v) Trivial.

(v) $\Rightarrow$ (iv) Suponha que $\Gamma \vdash \varphi$ e $\Gamma \vdash \neg\varphi$. A partir das duas derivações associadas a essas hipóteses, obtém-se uma derivação para $\Gamma \vdash \perp$ usando a regra $(\to E)$. $\square$

A cláusula (vi) nos diz por que razão conjuntos inconsistentes (ou teorias inconsistentes) são destituídas de interesse matemático. Pois, se tudo é derivável, não podemos distinguir entre "boas" e "más" proposições. A matemática tenta encontrar distinções, não borrá-las.

Na prática matemática procura-se estabelecer consistência exibindo-se um modelo (pense na consistência da negação do quinto postulado de Euclides e as geometrias não-euclideanas). No contexto da lógica proposicional isso significa procurar uma valoração apropriada.

**Lema 1.5.4** *Se existe uma valoração tal que* $[\![\psi]\!]_v = 1$ *para toda* $\psi \in \Gamma$*, então* $\Gamma$ *é consistente.*

*Demonstração.* Suponha que $\Gamma \vdash \bot$, então pelo Lema 1.5.1 $\Gamma \models \bot$, logo para qualquer valoração $v$ $[\![(\psi)]\!]_v = 1$ para toda $\psi \in \Gamma \Rightarrow [\![\bot]\!]_v = 1$. Como $[\![\bot]\!]_v = 0$ para todas as valorações, não existe valoração com $[\![\psi]\!]_v = 1$ para toda $\psi \in \Gamma$. Contradição. Portanto $\Gamma$ é consistente. □

*Exemplos.*

1. $\{p_0, \neg p_1, p_1 \to p_2\}$ é consistente. Uma valoração apropriada é uma que satisfaz $[\![p_0[\![= 1$, $[\![p_1]\!] = 0$.

2. $\{p_0, p_1, \ldots\}$ é consistente. Escolha a valoração constante 1.

A cláusula (v) do Lema 1.5.3 nos diz que $\Gamma \cup \{\varphi, \neg\varphi\}$ é inconsistente. Agora como poderia $\Gamma \cup \{\neg\varphi\}$ ser inconsistente? Parece plausível imputar isso à derivabilidade de $\varphi$. O próximo lema confirma isto.

**Lema 1.5.5** (a) $\Gamma \cup \{\neg\varphi\}$ *é inconsistente* $\Rightarrow \Gamma \vdash \varphi$*,*

(b) $\Gamma \cup \{\varphi\}$ *é inconsistente* $\Rightarrow \Gamma \vdash \neg\varphi$*.*

*Demonstração.* As suposições de (a) e de (b) permitem que se construam as duas derivações abaixo: ambas com conclusão $\bot$. Aplicando $(RAA)$, e $(\to I)$, obtemos derivações com hipóteses em $\Gamma$, de $\varphi$, e de $\neg\varphi$, respectivamente.

$$\dfrac{\begin{matrix}[\neg\varphi]\\ \mathcal{D}\\ \bot\end{matrix}}{\varphi}\,RAA \qquad\qquad \dfrac{\begin{matrix}[\varphi]\\ \mathcal{D}'\\ \bot\end{matrix}}{\neg\varphi}\to I$$

□

**Definição 1.5.6** Um conjunto $\Gamma$ é *maximamente consistente* sse

(a) $\Gamma$ é consistente,

(b) $\Gamma \subseteq \Gamma'$ e $\Gamma'$ consistente $\Rightarrow \Gamma = \Gamma'$.

*Observação.* Poder-se-ia substituir (b) por (b′): se $\Gamma$ é um subconjunto próprio de $\Gamma'$, então $\Gamma'$ é inconsistente. I.e., simplesmente acrescentando mais uma proposição, o conjunto torna-se inconsistente.

Conjuntos maximamente consistentes têm um papel importante em lógica. Mostraremos que existem muitos deles.

Aqui vai um exemplo: $\Gamma = \{\varphi \mid [\![\varphi]\!] = 1\}$ para uma valoração fixa. Pelo Lema 1.5.4 $\Gamma$ é consistente. Considere um conjunto consistente $\Gamma'$ tal que $\Gamma \subseteq \Gamma'$. Agora suponha que $\psi \in \Gamma'$ e que $[\![\psi]\!] = 0$, então $[\![\neg\psi]\!] = 1$, e portanto $\neg\psi \in \Gamma$.

Porém como $\Gamma \subseteq \Gamma'$ isso implica que $\Gamma'$ é inconsistente. Contradição. Por conseguinte $[\![\psi]\!] = 1$ para toda $\psi \in \Gamma'$, logo por definição $\Gamma = \Gamma'$. Da demonstração do Lema 1.5.11 segue que esse é basicamente o único tipo de conjunto maximamente consistente que podemos esperar.

O lema fundamental a seguir é demonstrado diretamente. O leitor pode reconhecer nele um análogo do Lema da Existência do Ideal Máximo da teoria dos anéis (ou o Teorema do Ideal Primo Booleano), que é usualmente demonstrado por uma aplicação do Lema de Zorn.

**Lema 1.5.7** *Cada conjunto consistente $\Gamma$ está contido em um conjunto maximamente consistente $\Gamma^*$.*

*Demonstração.* Existem um número contável de proposições, portanto suponha que temos uma lista $\varphi_0, \varphi_1, \varphi_2, \ldots$ de todas as proposições (cf. Exercício 5). Definimos uma seqüência não-decrescente de conjuntos $\Gamma_i$ tal que a união desses conjuntos é maximamente consistente.

$$
\begin{array}{lcl}
\Gamma_0 & = & \Gamma, \\
\Gamma_{n+1} & = & \begin{cases} \Gamma_n \cup \{\varphi_n\} \text{ se } \Gamma_n \cup \{\varphi_n\} \text{ é consistente,} \\ \Gamma_n \text{ caso contrário.} \end{cases} \\
\Gamma^* & = & \bigcup\{\Gamma_n \mid n \geq 0\}.
\end{array}
$$

(a) $\Gamma_n$ é consistente para todo $n$.

Imediato, por indução sobre $n$.

(b) $\Gamma^*$ é consistente.

Suponha que $\Gamma^* \vdash \perp$ então, pela definição de $\perp$ existe uma derivação $\mathcal{D}$ de $\perp$ com hipóteses em $\Gamma^*$; $\mathcal{D}$ tem um número finito de hipóteses $\psi_0, \ldots, \psi_k$. Como $\Gamma^* = \bigcup\{\Gamma_n \mid n \geq 0\}$, temos para cada $i \leq k$ $\psi_k \in \Gamma_{n_i}$ para algum $n_i$. Suponha que $n$ seja $\max\{n_i \mid i \leq k\}$, então $\psi_0, \ldots, \psi_k \in \Gamma_n$ e portanto $\Gamma_n \vdash \perp$. Mas $\Gamma$ é consistente. Contradição.

(c) $\Gamma^*$ é maximamente consistente. Suponha que $\Gamma^* \subseteq \Delta$ e que $\Delta$ seja consistente. Se $\psi \in \Delta$, então $\psi = \varphi_m$ para algum $m$. Como $\Gamma_m \subseteq \Gamma^* \subseteq \Delta$ e $\Delta$ é consistente, $\Gamma_m \cup \{\varphi_m\}$ é consistente. Por conseguinte $\Gamma_{m+1} = \Gamma_m \cup \{\varphi_m\}$, i.e. $\varphi_m \in \Gamma_{m+1} \subseteq \Gamma^*$. Isso mostra que $\Gamma^* = \Delta$. □

**Lema 1.5.8** *Se $\Gamma$ é maximamente consistente, então $\Gamma$ é fechado sob derivabilidade (i.e. $\Gamma \vdash \varphi \Rightarrow \varphi \in \Gamma$).*

*Demonstração.* Suponha que $\Gamma \vdash \varphi$ e que $\varphi \notin \Gamma$. Então $\Gamma \cup \{\varphi\}$ deve ser inconsistente. Portanto $\Gamma \vdash \neg\varphi$, logo $\Gamma$ é inconsistente. Contradição. □

**Lema 1.5.9** *Suponha que $\Gamma$ seja maximamente consistente; então*

(a) *para toda $\varphi$ ou $\varphi \in \Gamma$, ou $\neg\varphi \in \Gamma$,*

(b) *para todas $\varphi$, $\psi$ $\varphi \to \psi \in \Gamma \Leftrightarrow (\varphi \in \Gamma \Rightarrow \psi \in \Gamma)$.*

*Demonstração.* (a) Sabemos que não é possível que ambas $\varphi$ e $\neg\varphi$ pertençam a $\Gamma$. Considere $\Gamma' = \Gamma \cup \{\varphi\}$. Se $\Gamma'$ é inconsistente, então, por 1.5.5, 1.5.8, $\neg\varphi \in \Gamma$. Se $\Gamma'$ é consistente, então $\varphi \in \Gamma$ pela maximalidade de $\Gamma$.

(b) Suponha que $\varphi \to \psi \in \Gamma$ e que $\varphi \in \Gamma$. Vamos mostrar que: $\psi \in \Gamma$. Como $\varphi, \varphi \to \psi \in \Gamma$ e considerando que $\Gamma$ é fechado sob derivabilidade (Lema 1.5.8), obtemos que $\psi \in \Gamma$ por $\to E$.

Reciprocamente: Suponha que $\varphi \in \Gamma$ implica em $\psi \in \Gamma$. Se $\varphi \in \Gamma$ então obviamente $\Gamma \vdash \psi$, logo $\Gamma \vdash \varphi \to \psi$. Se $\varphi \notin \Gamma$, então $\neg\varphi \in \Gamma$, e portanto $\Gamma \vdash \neg\varphi$. Por conseguinte $\Gamma \vdash \varphi \to \psi$. □

Note que obtemos automaticamente o seguinte:

**Corolário 1.5.10** *Se $\Gamma$ é maximamente consistente, então $\varphi \in \Gamma \Leftrightarrow \neg\varphi \notin \Gamma$, e $\neg\varphi \in \Gamma \Leftrightarrow \varphi \notin \Gamma$.*

**Lema 1.5.11** *Se $\Gamma$ é consistente, então existe uma valoração tal que $[\![\psi]\!] = 1$ para toda $\psi \in \Gamma$.*

*Demonstração.* (a) Por 1.5.7 $\Gamma$ está contido em um $\Gamma^*$ maximamente consistente.

(b) Defina $v(p_i) = \begin{cases} 1 & \text{se } p_i \in \Gamma^* \\ 0 & \text{caso contrário} \end{cases}$ e estenda $v$ para a valoração $[\![\ ]\!]_v$.

Alegação: $[\![\varphi]\!] = 1 \Leftrightarrow \varphi \in \Gamma^*$. Use indução sobre $\varphi$.

1. Para $\varphi$ atômica a alegação se verifica por definição.

2. $\varphi = \psi \wedge \sigma$. $[\![\varphi]\!]_v = 1 \Leftrightarrow [\![\psi]\!]_v = [\![\sigma]\!]_v = 1 \Leftrightarrow$ (hipótese da indução) $\psi, \sigma \in \Gamma^*$ e portanto $\varphi \in \Gamma^*$. Reciprocamente, $\psi \wedge \sigma \in \Gamma^* \Leftrightarrow \psi, \sigma \in \Gamma^*$ (1.5.8). O restante segue da hipótese da indução.

3. $\varphi = \psi \to \sigma$. $[\![(\psi \to \sigma)]\!]_v = 0 \Leftrightarrow [\![\psi]\!]_v = 1$ e $[\![\sigma]\!]_v = 0 \Leftrightarrow$ (hipótese da indução) $\psi \in \Gamma^*$ e $\sigma \notin \Gamma^* \Leftrightarrow \psi \to \sigma \notin \Gamma^*$ (por 1.5.9).

(c) Como $\Gamma \subseteq \Gamma^*$ temos $[\![\psi]\!]_v = 1$ para toda $\psi \in \Gamma$. □

**Corolário 1.5.12** $\Gamma \nvdash \varphi \Leftrightarrow$ *existe uma valoração tal que $[\![\psi]\!] = 1$ para toda $\psi \in \Gamma$ e $[\![\varphi]\!] = 0$.*

*Demonstração.* $\Gamma \nvdash \varphi \Leftrightarrow \Gamma \cup \{\neg\varphi\}$ consistente $\Leftrightarrow$ existe uma valoração tal que $[\![\psi]\!] = 1$ para toda $\psi \in \Gamma \cup \{\neg\varphi\}$, ou $[\![\psi]\!] = 1$ para toda $\psi \in \Gamma$ e $[\![\psi]\!] = 0$. □

**Teorema 1.5.13 (Teorema da Completude)** $\Gamma \vdash \varphi \Leftrightarrow \Gamma \models \varphi$.

*Demonstração.* $\Gamma \nvdash \varphi \Rightarrow \Gamma \not\models \varphi$ por 1.5.12. A recíproca contrária se verifica por 1.5.1. □

Em particular temos $\vdash \varphi \Leftrightarrow\ \models \varphi$, logo o conjunto de teoremas é exatamente o conjunto de tautologias.

O Teorema da Completude nos diz que a tarefa tediosa de fazer derivações pode ser substituída pela tarefa (igualmente tediosa, porém automática) de checar tautologias. Em princípio isto simplifica consideravelmente a busca por teoremas; se, por um lado, para se construir derivações é preciso ser (razoavelmente) inteligente, por outro lado, para se montar tabelas-verdade é necessário se ter perseverança.

Para teorias lógicas às vezes se leva em conta uma outra noção de completude: uma conjunto $\Gamma$ é chamado de *completo* se para cada $\varphi$, $\Gamma \vdash \varphi$ ou $\Gamma \vdash \neg\varphi$. Essa noção é intimamente relacionada a "maximamente consistente". Do Exercício 6 segue que $Cons(\Gamma) = \{\sigma \mid \Gamma \vdash \sigma\}$ (o *conjunto de conseqüências de* $\Gamma$) é maximamente consistente se $\Gamma$ é um conjunto completo. A recíproca também se verifica (cf. Exercício 10). A própria lógica proposicional (i.e. o caso em que $\Gamma =$) não é completa nesse sentido, e.g. $\not{p}_0$ e $\vdash \neg p_0$.

Existe uma outra noção importante que é tradicionalmente levada em conta em lógica: *decidibilidade*. A lógica proposicional é decidível no seguinte sentido: existe um procedimento efetivo para verificar a derivabilidade de proposições $\varphi$. Colocando de outra forma: existe um algoritmo que para cada $\varphi$ testa se $\vdash \varphi$. O algoritmo é simples: escreva a tabela-verdade completa para $\varphi$ e verifique se a última coluna contém apenas 1's. Se for o caso, então $\models \varphi$ e, pelo Teorema da Completude, $\vdash \varphi$. Caso contrário, então $\not\models \varphi$ e portanto $\nvdash \varphi$. Esse certamente não é o melhor algoritmo, pode-se encontrar outros mais econômicos. Existem também algoritmos que dão mais informação, e.g. eles não apenas testam $\vdash \varphi$, mas também produzem uma derivação, se é que existe uma. Tais algoritmos, entretanto, requerem uma análise mais profunda de derivações. Isso está fora do escopo deste livro.

Há um aspecto do Teorema da Completude que desejamos discutir agora. Não vem como uma surpresa o fato de que verdade segue de derivabilidade. Afinal de contas começamos com uma noção combinatorial, definida indutivamente, e terminamos com 'ser verdadeiro para todas as valorações'. Uma demonstração indutiva simples resolve o problema.

Para a recíproca a situação é totalmente diferente. Por definição $\Gamma \models \varphi$ significa que $[\![\varphi]\!]_v = 1$ para todas as valorações $v$ que tornam verdadeiras as proposições de $\Gamma$. Portanto sabemos algo sobre o comportamento de *todas* as valorações com respeito a $\Gamma$ e $\varphi$. Podemos ter esperança de extrair desse número infinito de fatos conjuntistas a informação finita, concreta, necessária para construir uma derivação para $\Gamma \vdash \varphi$? Evidentemente os fatos disponíveis não nos dão muita coisa para prosseguir. Vamos portanto simplificar um pouco as coisas diminuindo o tamanho do conjunto $\Gamma$; afinal de contas usamos apenas um número finito de fórmulas de $\Gamma$ em uma derivação, portanto vamos supor que aquelas fórmulas $\psi_1, \ldots, \psi_n$ são dadas. Agora podemos esperar maior sucesso, pois apenas um número finito de átomos estão envolvidos, e por isso podemos considerar uma "parte" finita do número infinito de valorações que têm algum papel a desempenhar. Isso quer dizer que apenas as restrições das valorações ao conjunto dos átomos ocorrendo em $\psi_1, \ldots \psi_n, \varphi$ são relevantes. Vamos simplificar o problema ainda mais. Sabemos que $\psi_1, \ldots \psi_n \vdash \varphi$ $(\psi_1, \ldots \psi_n \models \varphi)$ pode ser substituído por $\vdash \psi_1 \wedge \ldots \wedge \psi_n \to \varphi$ $(\models \psi_1 \wedge \ldots \wedge \psi_n \to \varphi)$, baseando-se nas regras de derivação (a definição de valoração). Daí nos vem a pergunta: dada a tabela-verdade para uma tautologia $\sigma$, podemos efetivamente encontrar uma derivação para $\sigma$?

Essa questão não é respondida pelo Teorema da Completude, pois nossa demonstração não é efetiva (pelo menos não o é à primeira vista). A questão foi respondida positivamente, e.g. por Post, Bernays e Kalmar (cf. *Kleene* IV, §29) e foi facilmente tratada por meio das técnicas de Gentzen, ou por tableaux semânticos. Vamos apenas esquematizar um método de prova: podemos efetivamente encontrar uma forma normal conjuntiva $\sigma^*$ para $\sigma$ tal que $\vdash \sigma \leftrightarrow \sigma^*$.

Demonstra-se facilmente que $\sigma^*$ é uma tautologia se e somente se cada operando da conjunção contém um átomo e sua negação, ou $\neg\bot$, e junta-se todos para obter uma derivação de $\sigma^*$, que imediatamente resulta numa derivação de $\sigma$.

**Exercícios**

1. Verifique quais dos seguintes conjuntos são consistentes
   (a) $\{\neg p_1 \wedge p_2 \to p_0,\ p_1 \to (\neg p_1 \to p_2),\ p_0 \leftrightarrow \neg p_2\}$,
   (b) $\{p_0 \to p_1,\ p_1 \to p_2,\ p_2 \to p_3,\ p_3 \to \neg p_0\}$,
   (c) $\{p_0 \to p_1,\ p_0 \wedge p_2 \to p_1 \wedge p_3,\ p_0 \wedge p_2 \wedge p_4 \to p_1 \wedge p_3 \wedge p_5,\ \ldots\}$.

2. Mostre que as seguintes condições são equivalentes:
   (a) $\{\varphi_1, \ldots, \varphi_n\}$ é consistente.
   (b) $\nvdash \neg(\varphi_1 \wedge \varphi_2 \wedge \ldots \wedge \varphi_n)$.
   (c) $\nvdash \varphi_1 \wedge \varphi_2 \wedge \ldots \wedge \varphi_{n-1} \to \neg\varphi_n$.

3. $\varphi$ é *independente* de $\Gamma$ se $\Gamma \nvdash \varphi$ e $\Gamma \nvdash \neg\varphi$. Demonstre que: $p_1 \to p_2$ é independente de $\{p_1 \leftrightarrow p_0 \wedge \neg p_2, p_2 \to p_0\}$.

4. Um conjunto $\Gamma$ é *independente* se para cada $\varphi \in \Gamma$ $\Gamma - \{\varphi\} \nvdash \varphi$.

   (a) Demonstre que cada conjunto finito $\Gamma$ tem um subconjunto independente $\Delta$ tal que $\Delta \vdash \varphi$ para todo $\varphi \in \Gamma$.
   (b) Seja $\Gamma = \{\varphi_0, \varphi_1, \varphi_2, \ldots\}$. Encontre um conjunto equivalente $\Gamma' = \{\psi_0, \psi_1, \ldots\}$ (i.e. $\Gamma \vdash \psi_i$ e $\Gamma \vdash \varphi_i$ para todo $i$) tal que $\vdash \psi_{n+1} \to \psi_n$, mas $\nvdash \psi_n \to \psi_{n+1}$. Note que $\Gamma'$ pode ser finito.
   (c) Considere um conjunto infinito $\Gamma'$ como o do item (b). Defina $\sigma_0 = \psi_0$, $\sigma_{n+1} = \psi_n \to \psi_{n+1}$. Demonstre que $\Delta = \{\sigma_0, \sigma_1, \sigma_2, \ldots\}$ é independente e equivalente a $\Gamma'$.
   (d) Demonstre que cada conjunto $\Gamma$ é equivalente a um conjunto independente $\Delta$.
   (e) Demonstre que $\Delta$ não precisa ser um subconjunto de $\Gamma$ (considere $\{p_0, p_0 \wedge p_1, p_0 \wedge p_1 \wedge p_2, \ldots\}$).

5. Encontre uma maneira efetiva de enumerar todas as proposições (sugestão: considere conjuntos $\Gamma_n$ de todas as proposições de posto $\leq n$ com átomos vindos de $p_0, \ldots, p_n$).

6. Demonstre que um conjunto consistente $\Gamma$ é maximamente consistente se $\varphi \in \Gamma$ ou $\neg\varphi \in \Gamma$ para todo $\varphi$.

7. Demonstre que $\{p_0, p_1, p_2, \ldots, p_n, \ldots\}$ é completo.

8. (*Teorema da Compaccidade*). Demonstre que: existe um $v$ tal que $[\![\psi]\!]_v = 1$ para toda $\psi \in \Gamma \Leftrightarrow$ para cada subconjunto finito $\Delta \subseteq \Gamma$ existe um $v$ tal que $[\![\sigma]\!]_v = 1$ para toda $\sigma \in \Delta$.

   Formulada nos termos do Exercício 13 da seção 1.3: $[\![\Gamma]\!] \neq \emptyset$ se $[\![\Delta]\!] \neq \emptyset$ para todo $\Delta$ finito tal que $\Delta \subseteq \Gamma$.

9. Considere um conjunto infinito $\{\varphi_1, \varphi_2, \varphi_3, \ldots\}$. Se para cada valoração existe um $n$ tal que $[\![\varphi_n]\!] = 1$, então existe um $m$ tal que $\vdash \varphi_1 \vee \ldots \vee \varphi_m$. (Sugestão: considere as negações $\neg\varphi_1$, $\neg\varphi_2$, ..., e aplique o Exercício 8).

10. Demonstre que: $\mathrm{Cons}(\Gamma) - \{\sigma \mid \Gamma \vdash \sigma\}$ é um conjunto maximamente consistente $\Leftrightarrow$ $\Gamma$ é completo.

11. Demonstre que: $\Gamma$ é maximamente consistente $\Leftrightarrow$ existe uma única valoração tal que $[\![\psi]\!] = 1$ para toda $\psi \in \Gamma$, onde $\Gamma$ é uma teoria, i.e. $\Gamma$ é fechado sob $\vdash$ ($\Gamma \vdash \sigma \Rightarrow \sigma \in \Gamma$).

12. Seja $\varphi$ uma proposição contendo o átomo $p$. Por conveniência escrevemos $\varphi(\sigma)$ para designar $\varphi[\sigma/p]$. Tal qual anteriormente, abreviamos $\neg\bot$ por $\top$.

    Demonstre que: $(i)$ $\varphi(\top) \vdash \varphi(\top) \leftrightarrow \top$ e $\varphi(\top) \vdash \varphi(\varphi(\top))$.
    $(ii)$ $\neg\varphi(\top) \vdash \varphi(\top) \leftrightarrow \bot$,
    $\varphi(p), \neg\varphi(\top) \vdash p \leftrightarrow \bot$,
    $\varphi(p), \neg\varphi(\top) \vdash \varphi(\varphi(\top))$.
    $(iii)$ $\varphi(p) \vdash \varphi(\varphi(\top))$.

13. Se os átomos $p$ e $q$ não ocorrem em $\psi$ e $\varphi$ respectivamente, então

    $\models \varphi(p) \to \psi \Rightarrow \models \varphi(\sigma) \to \psi$ para toda $\sigma$,

    $\models \varphi \to \psi(q) \Rightarrow \models \varphi \to \psi(q)$ para toda $\sigma$.

14. Suponha que $\vdash \varphi \to \psi$. Chamamos $\sigma$ de *interpolante* se $\vdash \varphi \to \sigma$ e $\vdash \sigma \to \psi$, e além disso $\sigma$ contém apenas átomos comuns a $\varphi$ e $\psi$. Considere $\varphi(p, r)$, $\psi(r, q)$ com todos os átomos à mostra. Demonstre que $\varphi(\varphi(\top, r), r)$ é um interpolante (use os Exercícios 12, 13).

15. Demonstre o *Teorema da Interpolação* (Craig): Para qualquer $\varphi$, $\psi$ com $\vdash \varphi \to \psi$ existe um interpolante (faça repetidamente o procedimento do Exercício 13).

## 1.6 Os conectivos que faltam

A linguagem da seção 1.4 continha apenas os conectivos $\wedge$, $\to$ e $\bot$. Nós já sabemos que, do ponto de vista semântico, essa linguagem é suficientemente rica, ou seja, os conectivos que faltam podem ser definidos em função dos que dispomos. Na verdade já usamos, nas seções precedentes, a negação como uma noção definida.

É uma questão de prática matemática segura se introduzir novas noções se seu uso simplifica nosso trabalho, e se elas codificam prática informal corrente. Isso, claramente, é uma razão para se introduzir $\neg$, $\leftrightarrow$ e $\vee$.

Agora existem duas maneiras de proceder: pode-se introduzir os novos conectivos como abreviações (de proposições complicadas), ou pode-se enriquecer a linguagem adicionando-se de fato os conectivos ao alfabeto, e fornecendo-se as respectivas regras de derivação.

O primeiro procedimento foi adotado acima; trata-se de procedimento completamente inofensivo, como por exemplo, a cada vez que se lê $\varphi \leftrightarrow \psi$ deve-se substituir por $(\varphi \to \psi) \wedge (\psi \to \varphi)$. Portanto não é nada mais que uma abreviação, introduzida por conveniência. O segundo procedimento é de natureza mais teórica. A linguagem é enriquecida e o conjunto de derivações é expandido. Como conseqüência é preciso que se reveja os resultados teóricos (tal como o Teorema da Completude) obtidos para a linguagem mais simples.

Adotaremos o primeiro procedimento porém esboçaremos também a segunda abordagem.

**Definição 1.6.1**

$$\begin{aligned} \varphi \vee \psi &:= \neg(\neg\varphi \vee \neg\psi), \\ \neg\varphi &:= \varphi \to \perp, \\ \varphi \leftrightarrow \psi &:= (\varphi \to \psi) \wedge (\psi \to \varphi). \end{aligned}$$

Obs.: Isso significa que as expressões acima *não* fazem parte da linguagem, mas são abreviações para certas proposições.

As propriedades de $\vee$, $\neg$ e $\leftrightarrow$ são dadas a seguir:

**Lema 1.6.2**
*(i)* $\varphi \vdash \varphi \vee \psi$, $\psi \vdash \varphi \vee \psi$,
*(ii)* $\Gamma, \varphi \vdash \sigma$ *e* $\Gamma, \psi \vdash \sigma \Rightarrow \Gamma, \varphi \vee \psi \vdash \sigma$,
*(iii)* $\varphi, \neg\varphi \vdash \perp$,
*(iv)* $\Gamma, \varphi \vdash \perp \Rightarrow \Gamma \vdash \neg\varphi$,
*(v)* $\varphi \leftrightarrow \psi$, $\varphi \vdash \psi$ *e* $\varphi \leftrightarrow \psi, \psi \vdash \varphi$,
*(vi)* $\Gamma, \varphi \vdash \psi$ *e* $\Gamma, \psi \vdash \varphi \Rightarrow \Gamma \vdash \varphi \leftrightarrow \psi$.

*Demonstração.* A única parte não trivial é (ii). Exibimos uma derivação de $\sigma$ a partir de $\Gamma$ e $\varphi \vee \psi$ (i.e. $\neg(\neg\varphi \vee \neg\psi)$), dadas derivações $\mathcal{D}_1$ e $\mathcal{D}_2$ de $\Gamma, \varphi \vdash \sigma$ e $\Gamma, \psi \vdash \sigma$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\begin{matrix}\Gamma, [\varphi]^1 \\ \mathcal{D}_1 \\ \sigma\end{matrix} \qquad [\neg\sigma]^3}{\perp}\to E}{\neg\varphi}\to I_1 \qquad \dfrac{\dfrac{\begin{matrix}\Gamma, [\psi]^2 \\ \mathcal{D}_2 \\ \sigma\end{matrix} \qquad [\neg\sigma]^3}{\perp}\to E}{\neg\psi}\to I_2}{\neg\varphi \wedge \neg\psi}\wedge I \qquad \neg(\neg\varphi \vee \neg\psi)}{\perp}\to E}{\sigma}\mathrm{RAA}_3$$

Os casos restantes deixo ao leitor. □

Note que (i) e (ii) podem ser lidos como regras de introdução e eliminação para $\vee$, (iii) e (iv) a mesma coisa para $\neg$, (vi) e (v) também para $\leftrightarrow$.

Tais propriedades legalizam as seguintes abreviações em derivações:

$$\dfrac{\varphi}{\varphi \vee \psi}\vee I \qquad \dfrac{\psi}{\varphi \vee \psi}\vee I \qquad\qquad \dfrac{\varphi \vee \psi \qquad \begin{matrix}[\varphi] \\ \vdots \\ \sigma\end{matrix} \qquad \begin{matrix}[\psi] \\ \vdots \\ \sigma\end{matrix}}{\sigma}\vee E$$

$$\dfrac{\begin{matrix}[\varphi]\\ \vdots \\ \bot\end{matrix}}{\neg\varphi}\neg I \qquad\qquad \dfrac{\varphi \quad \neg\varphi}{\bot}\neg E$$

$$\dfrac{\begin{matrix}[\varphi]\\ \vdots\\ \psi\end{matrix}\qquad \begin{matrix}[\psi]\\ \vdots\\ \psi\end{matrix}}{\varphi\leftrightarrow\psi}\leftrightarrow I \qquad\qquad \dfrac{\varphi \quad \varphi\leftrightarrow\psi}{\psi}\quad\dfrac{\varphi\quad\varphi\leftrightarrow\psi}{\psi}\leftrightarrow E$$

Considere por exemplo a seguinte aplicação de $\vee E$

$$\dfrac{\begin{matrix}\mathcal{D}_0\\ \varphi\vee\psi\end{matrix}\qquad \begin{matrix}[\varphi]\\ \mathcal{D}_1\\ \sigma\end{matrix}\qquad\begin{matrix}[\psi]\\ \mathcal{D}_2\\ \sigma\end{matrix}}{\sigma}\vee E$$

Trata-se de mera abreviação para

$$\dfrac{\dfrac{\begin{matrix}\mathcal{D}_0\\ \neg(\neg\varphi\wedge\neg\psi)\end{matrix}\qquad \dfrac{\dfrac{\dfrac{\begin{matrix}[\varphi]^1\\ \mathcal{D}_1\\ \sigma\end{matrix}\quad[\neg\sigma]^3}{\bot}}{\neg\varphi}1\qquad \dfrac{\dfrac{\begin{matrix}[\psi]^2\\ \mathcal{D}_2\\ \sigma\end{matrix}\quad[\neg\sigma]^3}{\bot}}{\neg\psi}2}{\neg\varphi\wedge\neg\psi}}{\bot}}{\sigma}3$$

O leitor está convocado a usar as abreviações acima em derivações reais, sempre que for conveniente. Via de regra, apenas $\vee I$ e $\vee E$ são de alguma importância, e leitor terá obviamente reconhecido as regras para $\neg$ e $\leftrightarrow$ como aplicações ligeiramente excêntricas de regras familiares.

*Exemplos.* $\vdash (\varphi\vee\psi)\vee\sigma\leftrightarrow(\varphi\vee\sigma)\wedge(\psi\vee\sigma)$.

$$\dfrac{\dfrac{(\varphi\wedge\psi)\vee\sigma\quad \dfrac{\dfrac{[\varphi\wedge\psi]^1}{\varphi}}{\varphi\vee\sigma}\quad\dfrac{[\sigma]^1}{\varphi\vee\sigma}}{\varphi\vee\sigma}1\qquad \dfrac{(\varphi\wedge\psi)\vee\sigma\quad\dfrac{\dfrac{[\varphi\wedge\psi]^2}{\psi}}{\psi\vee\sigma}\quad\dfrac{[\sigma]^2}{\psi\vee\sigma}}{\psi\vee\sigma}2}{(\varphi\vee\sigma)\wedge(\psi\vee\sigma)} \tag{1}$$

Reciprocamente

$$\dfrac{\dfrac{(\varphi\vee\sigma)\wedge(\psi\vee\sigma)}{\varphi\vee\sigma} \qquad \dfrac{\dfrac{(\varphi\vee\sigma)\wedge(\psi\vee\sigma)}{\psi\vee\sigma} \qquad \dfrac{\dfrac{[\varphi]^2 \quad [\psi]^1}{\varphi\wedge\psi}}{(\varphi\wedge\psi)\vee\sigma} \qquad \dfrac{[\sigma]^1}{(\varphi\wedge\psi)\vee\sigma}}{(\varphi\wedge\psi)\vee\sigma}\,1 \qquad \dfrac{[\sigma]^2}{(\varphi\wedge\psi)\vee\sigma}}{(\varphi\wedge\psi)\vee\sigma}\,2$$

(2)

Combinando (1) e (2) obtemos a seguinte derivação:

$$\dfrac{\begin{array}{c}[(\varphi\wedge\psi)\vee\sigma]\\ \mathcal{D}\\ (\varphi\vee\sigma)\wedge(\psi\vee\sigma)\end{array} \qquad \begin{array}{c}[(\varphi\wedge\psi)\vee\sigma]\\ \mathcal{D}'\\ (\varphi\wedge\psi)\vee\sigma\end{array}}{(\varphi\wedge\psi)\vee\sigma\leftrightarrow(\varphi\vee\sigma)\wedge(\psi\vee\sigma)}\leftrightarrow I$$

$\vdash \varphi\vee\neg\varphi$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\varphi]^1}{\varphi\vee\neg\varphi}\vee I \qquad [\neg(\varphi\vee\neg\varphi)]^2}{\bot}\to E}{\neg\varphi}\to I_1}{\varphi\vee\neg\varphi}\vee I \qquad [\neg(\varphi\vee\neg\varphi)]^2}{\bot}\to E}{\varphi\vee\neg\varphi}\,\mathrm{RAA}_2$$

$\vdash (\varphi\to\psi)\vee(\psi\to\varphi)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\varphi]^1}{\psi\to\varphi}\to I_1}{(\varphi\to\psi)\vee(\psi\to\varphi)}\vee I \qquad [\neg((\varphi\to\psi)\vee(\psi\to\varphi))]^2}{\bot}\to E}{\psi}\,\bot}{\varphi\to\psi}\to I_1}{(\varphi\to\psi)\vee(\psi\to\varphi)}\vee I \qquad [\neg((\varphi\to\psi)\vee(\psi\to\varphi))]^2}{\bot}\to E}{(\varphi\to\psi)\vee(\psi\to\varphi)}\,\mathrm{RAA}_2$$

$\vdash \neg(\varphi \wedge \psi) \to \neg\varphi \vee \neg\psi$

$$\dfrac{\dfrac{\dfrac{[\neg(\varphi\wedge\psi)] \qquad \dfrac{\dfrac{\dfrac{[\neg(\neg\varphi\vee\neg\psi)] \quad \dfrac{[\neg\varphi]}{\neg\varphi\vee\neg\psi}}{\perp}}{\varphi} \qquad \dfrac{\dfrac{[\neg(\neg\varphi\vee\neg\psi)] \quad \dfrac{[\neg\psi]}{\neg\varphi\vee\neg\psi}}{\perp}}{\psi}}{\varphi\wedge\psi}}{\perp}}{\neg\varphi\vee\neg\psi}}{\neg(\varphi\wedge\psi)\to(\neg\varphi\vee\neg\psi)}$$

□

Agora vamos dar uma idéia de como seria a segunda abordagem. Adicionamos $\vee$, $\neg$ e $\leftrightarrow$ à linguagem, e consequentemente extendemos o conjunto de proposições. Em seguida adicionamos as regras para $\vee$, $\neg$ e $\leftrightarrow$ relacionadas acima ao nosso estoque de regras de derivação. Para ser mais precisos, nesse ponto deveríamos também introduzir um novo símbolo de derivabilidade, porém continuaremos a usar o já estabelecido $\vdash$ na esperança de que o leitor se lembrará que agora estamos fazendo derivações em um sistema maior. As seguintes condições se verificam:

**Teorema 1.6.3**
$\vdash \varphi \vee \psi \leftrightarrow \neg(\neg\varphi \wedge \neg\psi)$.
$\vdash \neg\varphi \leftrightarrow (\varphi \to \perp)$.
$\vdash (\varphi \leftrightarrow \psi) \leftrightarrow (\varphi \to \psi) \wedge (\psi \to \varphi)$.

*Demonstração.* Observe que, pelo Lema 1.6.2, os conectivos definidos e os primitivos (estes os 'reais' conectivos) obedecem a exatamente as mesmas relações de derivabilidade (regras de derivação, se você prefere). Isso nos leva imediamente ao resultado desejado. Vamos dar um exemplo.

$\varphi \vdash \neg(\neg\varphi \wedge \neg\psi)$ e $\psi \vdash \neg(\neg\varphi \wedge \neg\psi)$ (1.6.2(i)), logo por $\vee E$ obtermos
$\varphi \vee \psi \vdash \neg(\neg\varphi \vee \neg\psi) \ldots (1)$
Reciprocamente, $\varphi \vdash \varphi \vee \psi$ (por $\vee I$), logo por 1.6.2(ii)
$\neg(\neg\varphi \vee \neg\psi) \vdash \varphi \vee \psi \ldots (2)$
Aplique $\leftrightarrow I$ a (1) e (2), então $\vdash \varphi \vee \psi \leftrightarrow \neg(\neg\varphi \wedge \neg\psi)$. O resto deixo ao leitor. □

Para ver mais resultados direciono o leitor aos exercícios.

As regras para $\vee$, $\leftrightarrow$, e $\neg$ capturam de fato o significado intuitivo daqueles conectivos. Vamos considerar a disjunção: $(\vee I)$: Se sabemos que $\varphi$ se verifica então certamente sabemos que $\varphi \vee \psi$ se verifica (sabemos até qual dos dois operandos se verifica). A regra $(\vee E)$ captura a idéia da "prova por casos": se sabemos que $\varphi \vee \psi$ se verifica e em cada um dos dois casos podemos concluir que $\sigma$ se verifica, então podemos imediatamente concluir que $\sigma$ se verifica. A disjunção intuitivamente pede uma decisão: qual dos dois operandos é dado ou pode ser suposto? Esse traço construtivo de $\vee$ fica grosseiramente (mesmo que convenientemente) apagado pela identificação de $\varphi \vee \psi$ e $\neg(\neg\varphi \vee \neg\psi)$. Essa última fórmula apenas nos diz que $\varphi$ e $\psi$ não podem estar ambas erradas, porém não diz qual das duas é correta. Para maiores informações sobre essa questão de construtividade, que tem um papel importante na demarcação da fronteira entre lógica clássica bi-valorada e lógica intuicionística efetiva, remeto o leitor ao Capítulo 5.

Note que com $\vee$ como um conectivo primitivo alguns teoremas tornam-se mais difíceis de provar. E.g. $\vdash \neg(\neg\neg\varphi \wedge \neg\varphi)$ é trivial, mas $\vdash \varphi \vee \neg\varphi$ não é. A seguinte regra geral pode ser útil: passar de premissas não-efetivas (ou nenhuma) para uma conclusão efetiva pede por uma aplicação de $RAA$.

### Exercícios

1. Demonstre usando dedução natural que $\vdash \varphi \vee \psi \rightarrow \psi \vee \varphi$, $\vdash \varphi \vee \varphi \leftrightarrow \varphi$.

2. Considere a linguagem cheia $\mathcal{L}$ com todos os conectivos $\wedge$, $\rightarrow$, $\perp$, $\leftrightarrow$, $\vee$ e a linguagem restrita $\mathcal{L}'$ com os conectivos $\wedge$, $\rightarrow$, $\perp$. Usando as regras de derivação apropriadas obtemos as noções de derivabilidade $\vdash$ e $\vdash'$. Definimos uma tradução óbvia de $\mathcal{L}$ para $\mathcal{L}'$:

$$\begin{array}{rcl}
\varphi^+ & := & \varphi, \text{ para } \varphi \text{ atômica} \\
(\varphi \Box \psi)^+ & := & \varphi^+ \Box \psi^+ \text{ para } \Box = \wedge, \rightarrow, \\
(\varphi \vee \psi)^+ & := & \neg(\neg\varphi^+ \wedge \neg\psi^+), \text{ onde } \neg \text{ é uma abreviação}, \\
(\varphi \leftrightarrow \psi)^+ & := & (\varphi^+ \rightarrow \psi^+) \wedge (\psi^+ \rightarrow \varphi^+), \\
(\neg\varphi)^+ & := & \varphi^+ \rightarrow \perp.
\end{array}$$

Demonstre que

$(i)$ $\vdash \varphi \leftrightarrow \varphi^+$,
$(ii)$ $\vdash \varphi \Leftrightarrow \vdash' \varphi^+$,
$(iii)$ $\varphi^+ = \varphi$ para $\varphi \in \mathcal{L}'$.
$(iv)$ A lógica cheia é *conservativa* em relação à lógica restrita, isto é, para $\varphi \in \mathcal{L}'$ $\vdash \varphi \Leftrightarrow \vdash' \varphi$.

3. Demonstre que o Teorema da Completude se verifica para a lógica cheia. Sugestão: use o Exercício 2.

4. Demonstre que
   $(a)$ $\vdash \top \vee \perp$.
   $(b)$ $\vdash (\varphi \leftrightarrow \top) \vee (\varphi \leftrightarrow \perp)$.
   $(c)$ $\vdash \varphi \leftrightarrow (\varphi \leftrightarrow \top)$.

5. Demonstre que $\vdash (\varphi \vee \psi) \leftrightarrow ((\varphi \rightarrow \psi) \rightarrow \psi)$.

6. Demonstre que:
   (a) $\Gamma$ é completa $\Leftrightarrow$ ($\Gamma \vdash \varphi \vee \psi \Leftrightarrow \Gamma \vdash \varphi$ ou $\Gamma \vdash \psi$, para toda $\varphi$, $\psi$),
   (b) $\Gamma$ é maximamente consistente $\Leftrightarrow$ $\Gamma$ é uma teoria consistente e para toda $\varphi$, $\psi$ ($\varphi \vee \psi \in \Gamma \Leftrightarrow \varphi \in \Gamma$ ou $\psi \in \Gamma$).

7. Demonstre que no sistema com $\vee$ como um conectivo primitivo:
   $\vdash (\varphi \rightarrow \psi) \leftrightarrow (\neg\varphi \vee \psi)$,
   $\vdash (\varphi \rightarrow \psi) \vee (\psi \rightarrow \varphi)$.

# Capítulo 2

# Lógica de Predicados

## 2.1 Quantificadores

Na lógica proposicional usamos porções grandes da linguagem matemática, a saber aquelas partes que podem ter um valor-verdade. Infelizmente, esse uso da linguagem é claramente insuficiente para a prática matemática. Um simples argumento, tal como "todos os quadrados são positivos, 9 é um quadrado, por conseguinte 9 é positivo" não pode ser tratado. Do ponto de vista proposicional a sentença acima é da forma $\varphi \wedge \psi \to \sigma$, e não há razão para que essa sentença (codificada) seja verdadeira, embora que obviamente aceitamos como verdadeira a sentença original. O moral da estória é que temos que estender a linguagem de modo que possamos discorrer sobre objetos e relações. Em particular desejamos introduzir meios de falar sobre *todos* os objetos do domínio de discurso, e.g. queremos permitir enunciados da forma "todos os números pares são resultado de uma soma de dois números primos ímpares". De forma dual, desejamos dispor de meios para expressar "existe um objeto tal que ...", e.g. no enunciado "existe um número real cujo quadrado é 2".

A experiência tem nos ensinado que os enunciados matemáticos básicos são da forma "$a$ tem a propriedade $p$" ou "$a$ e $b$ estão na relação $R$", etc. Exemplos disso são: "$n$ é par", "$f$ é diferenciável", "$3 = 5$", "$7 < 12$", "$B$ está entre $A$ e $C$". Por conseguinte construimos nossa linguagem a partir de símbolos para *propriedades*, *relações* e *objetos*. Além disso adicionamos *variáveis* que recebem objetos como valores (as chamadas variáveis individuais), e os conectivos lógicos usuais agora incluindo os *quantificadores* $\forall$ e $\exists$ (para representar "para todo" e "existe").

Primeiramente vamos dar alguns exemplos informais.

| | | |
|---|---|---|
| $\exists x P(x)$ | – | existe um $x$ com propriedade $P$, |
| $\forall y P(y)$ | – | para todo $y$ $P$ se verifica (todo $y$ tem a propriedade $P$), |
| $\forall x \exists y(x = 2y)$ | – | para todo $x$ existe um $y$ tal que $x$ é o dobro de $y$, |
| $\forall \varepsilon(\varepsilon > 0 \rightarrow \exists n(\frac{1}{n} < \varepsilon))$ | – | para todo $\varepsilon$ positivo existe um $n$ tal que $\frac{1}{n} < \varepsilon$, |
| $x < y \rightarrow \exists z(x < z \wedge z < y)$ | – | se $x < y$, então existe um $z$ tal que $x < z$ e $z < y$, |
| $\forall x \exists y(x.y = 1)$ | – | para cada $x$ existe um inverso $y$. |

Sabemos da teoria elementar dos conjuntos que funções são tipos especiais de relações. Entretanto, seria um flagrante conflito com a prática matemática evitar funções (ou mapeamentos). Além do mais, seria extremamente incômodo. Portanto vamos incorporar funções em nossa linguagem.

Grosso modo a linguagem lida com duas categorias de entidades sintáticas: uma para objetos - os *termos*, uma para enunciados - as *fórmulas*. Exemplos de termos são: 17, $x$, $(2 + 5) - 7$, $x^{3y+1}$.

De que é que fala a lógica de predicados com uma certa linguagem? Ou, em outras palavras, os termos e as fórmulas falam de quê? A resposta é: fórmulas podem expressar propriedades relativas a um dado conjunto de relações e funções sobre um determinado domínio de discurso. Já encontramos tais situações em matemática; falamos sobre *estruturas*, e.g. grupos, anéis, módulos, conjuntos ordenados (consulte um texto de álgebra). Faremos de estruturas nosso ponto de partida e voltaremos à lógica mais adiante.

Em nossa lógica falaremos sobre "todos os números" ou "todos os elementos", mas não sobre "todos os ideais" ou "todos os subconjuntos", etc. Em geral nossas variáveis terão seus valores variando sobre elementos de um dado universo (e.g. as matrizes $n \times n$ sobre os reais), mas não sobre propriedades ou relações, ou propriedades de propriedades, etc. Por essa razão a lógica de predicados desse livro é chamada de *lógica de primeira ordem*, ou também *lógica elementar*. Na prática da matemática, e.g. em análise, usa-se lógica de alta ordem. Num certo sentido é surpreendente que a lógica de primeira ordem possa fazer tanto pela matemática, como veremos adiante. Uma breve introdução à lógica de segunda ordem será apresentada no capítulo 4.

## 2.2 Estruturas

Um grupo é um conjunto (não-vazio) equipado com duas operações, uma binária e uma unária, e com um elemento neutro (satisfazendo certas leis). Um conjunto parcialmente ordenado é um conjunto, equipado com uma relação binária (satisfazendo certas leis).

Generalizamos isso da seguinte forma:

**Definição 2.2.1** Uma *estrutura* é uma seqüência ordenada $\langle A, R_1, \ldots, R_n, F_1, \ldots, F_m, \{c_i \mid i \in I\}\rangle$, onde $A$ é um conjunto não-vazio. $R_1, \ldots, R_n$ são *relações* sobre $A$, $F_1, \ldots, F_m$ são *funções* sobre $A$, os $c_i$'s ($i \in I$) são os elementos de $A$ (*constantes*).

*Advertência.* As funções $F_i$ são *totais*, i.e. definidas para todo os valores de entrada; isso às vezes pede a utilização de alguns truques, tal como com $0^{-1}$ (cf. a definição de anéis mais adiante).

*Exemplos.* $\langle \mathbb{R}, +, \cdot, ^{-1}, 0, 1\rangle$ – o corpo dos números reais,
$\langle \mathbb{N}, <\rangle$ – o conjunto ordenado dos números naturais.

Designamos estruturas por meio de letras góticas maiúsculas: $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, ....

Se por um momento esquecermos as propriedades especiais das relações e operações (e.g. comutatividade da adição sobre os reais), então o que resta é o *tipo* de uma estrutura, que é dado pelo número de relações, funções (ou operações), e seus respectivos argumentos, mais o número (cardinalidade) de constantes.

**Definição 2.2.2** O *tipo de similaridade* de uma estrutura $\mathfrak{A} = \langle A, R_1, \ldots, R_n, F_1, \ldots, F_m, \{c_i \mid i \in I\}\rangle$ é uma seqüência, $\langle r_1, \ldots, r_n; a_1, \ldots, a_m; \kappa\rangle$, onde $R_i \subseteq A^{r_i}$, $F_j : A^{a_j} \to A$, $\kappa = |\{c_i \mid i \in I\}|$ (cardinalidade de $I$).

As duas estruturas no nosso exemplo têm tipo de similaridade $\langle -; 2, 2, 1; 2\rangle$ e $\langle 2; -; 0\rangle$. A ausência de relações, funções é indicada por $-$. Não há objeção a estender a noção de estrutura para conter um número arbitrariamente grande de relações ou funções, mas as estruturas mais comuns têm tipos finitos (incluindo um número finito de constantes).

Obviamente, teria sido melhor usar notações similares para nossas estruturas, i.e. $\langle A; R_1, \ldots, R_n; f_1, \ldots, F_m; \{c_i \mid i \in I\}\rangle$, mas seria demasiadamente pedante.

Se $R \subseteq A$, então dizemos que $R$ é uma propriedade (ou *relação unária*); se $R \subseteq A^2$ dizemos que $R$ é uma *relação binária*; se $R \subseteq A^n$, dizemos que $R$ é uma *relação n-ária*.

O conjunto $A$ é chamado de *universo* de $\mathfrak{A}$.

*Notação.* $A = |\mathfrak{A}|$.

$\mathfrak{A}$ é dita (in)finita se seu universo é (in)finito. Frequentemente cometeremos um pequeno abuso de linguagem escrevendo as constantes ao invés do conjunto de constantes, como no exemplo do corpo dos números reais no qual deveríamos ter escrito: $\langle \mathbb{R}, +, \cdot, ^{-1}, \{0, 1\}\rangle$, porém $\langle \mathbb{R}, +, \cdot, ^{-1}, 0, 1\rangle$ é mais tradicional. Entre as relações que encontramos em estruturas, existe uma muito especial: a *relação de identidade* (ou *de igualdade*).

Visto que, via de regra, estruturas matemáticas são equipadas com a relação de identidade, não listamos essa relação separadamente. Portanto, ela não aparece no tipo de similaridade. Daqui por diante assumimos que todas as estruturas possuem uma relação de identidade, e mencionaremos explicitamente quaisquer exceções. Para investigações puramente lógicas, é óbvio que faz sentido considerar uma lógica sem a identidade, mas este livro serve a leitores das comunidades de matemática e de ciência da computação.

Considera-se também os "casos limite" de relações e funções, i.e. relações e funções 0-árias. Uma relação 0-ária é um subconjunto de $A^{\emptyset}$. Como $A^{\emptyset} = \{\emptyset\}$ existem duas dessas relações: $\emptyset$ e $\{\emptyset\}$ (consideradas como ordinais: 0 e 1). Relações 0-árias podem portanto ser vistas como valores-verdade, o que faz com que elas desempenhem o papel das interpretações de proposições. Na prática as relações 0-árias não aparecem, e.g. elas não têm qualquer função em álgebra. A maior parte do tempo o leitor pode prazerosamente esquecê-las, embora que ainda assim vamos permitir tais relações em nossa definição porque elas simplificam certas considerações. Uma função 0-ária é um mapeamento de $\{\emptyset\}$ para $A$. Como o mapeamento tem um conjunto unitário como domínio, podemos considerá-lo como igual à sua imagem.

Dessa forma, funções 0-árias podem fazer o papel das constantes. A vantagem desse procedimento é, no entanto, desprezível no presente contexto, portanto manteremos nossas constantes.

**Exercícios**

1. Escreva o tipo de similaridade das seguintes estruturas:
   (i) $\langle \mathbb{Q}, <, 0\rangle$
   (ii) $\langle \mathbb{N}, +, \cdot, S, 0, 1, 2, 3, 4, \ldots, n, \ldots\rangle$, onde $S(x) = x + 1$,
   (iii) $\langle \mathcal{P}(\mathbb{N}), \subseteq, \cup, \cap, ^c, \emptyset\rangle$,
   (iv) $\langle \mathbb{Z}/5, +, \cdot, -, ^{-1}, 0, 1, 2, 3, 4\rangle$,
   (v) $\langle \{0, 1\}, \wedge, \vee, \rightarrow, \neg, 0, 1\rangle$, onde $\wedge$, $\vee$, $\rightarrow$, $\neg$ operam de acordo com as tabelas-verdade usuais,
   (vi) $\langle \mathbb{R}, 1\rangle$,
   (vii) $\langle \mathbb{R}\rangle$,
   (viii) $\langle \mathbb{R}, \mathbb{N}, <, T, ^2, |\ |, -\rangle$, onde $T(a, b, c)$ é a relação '$b$ está entre $a$ e $c$', $^2$ é a função 'eleva ao quadrado', $-$ é a função de subtração e $|\ |$ a função valor absoluto.

2. Dê estruturas com tipo de similaridade $\langle 1, 1; -; 3\rangle$, $\langle 4; -; 0\rangle$.

## 2.3 A Linguagem de um Tipo de Similaridade

As considerações desta seção são generalizações daquelas da seção 1.1.1. Como os argumentos são bastante semelhantes, deixaremos um bom número de detalhes a cargo do leitor. Por conveniência fixamos o tipo de similaridade nesta seção: $\langle r_1, \ldots, r_n; a_1, \ldots, a_m; \kappa\rangle$, onde assumimos que $r_i \geq 0$, $a_j > 0$.

O alfabeto consiste dos seguintes símbolos:

| | | |
|---|---|---|
| 1. | Símbolos de predicado: | $P_1, \ldots, P_n, \dot{=}$ |
| 2. | Símbolos de função: | $f_1, \ldots, f_m$ |
| 3. | Símbolos de constante: | $\overline{c}_i$ para $i \in I$ |
| 4. | Variáveis: | $x_0, x_1, x_2, \ldots$ (um número contável delas) |
| 5. | Conectivos: | $\vee, \wedge, \rightarrow, \neg, \leftrightarrow, \perp, \forall, \exists$ |
| 6. | Símbolos auxiliares: | (, ). |

$\forall$ e $\exists$ são chamados de *quantificador universal* e *quantificador existencial*. O símbolo de igualdade de curiosa aparência (com um ponto em cima) foi escolhido para evitar possíveis confusões, pois existem na verdade vários símbolos de igualdade em uso: um para indicar a identidade nos modelos, um para indicar a igualdade na meta-linguagem, e o sintático introduzido acima. Praticaremos, no entanto, o costumeiro abuso de linguagem, e usaremos essas distinções apenas se for realmente necessária. Via de regra o leitor não terá dificuldade em reconhecer o tipo de identidade envolvida.

A seguir definimos as duas categorias sintáticas.

**Definição 2.3.1** $TERM$ é o menor conjunto $X$ com as seguintes propriedades:
(i) $\overline{c}_i \in X$ $(i \in I)$ e $x_i \in X$ $(i \in \mathbb{N})$,
(ii) $t_1, \ldots, t_{a_i} \in X \Rightarrow f_i(t_1, \ldots, t_{a_i}) \in X$, para $1 \leq i \leq m$

$TERM$ é o nosso *conjunto de termos*.

**Definição 2.3.2** $FORM$ é o menor conjunto $X$ com as seguintes propriedades:
(i) $\perp \in X$; $P_i \in X$ se $r_i = 0$; $t_1, \ldots, t_{r_i} \in TERM \Rightarrow$
$P_i(t_1, \ldots, t_{r_i}) \in X$; $t_1, t_2 \in TERM \Rightarrow t_1 = t_2 \in X$,
(ii) $\varphi, \psi \in X \Rightarrow (\varphi \Box \psi) \in X$ onde $\Box \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$,
(iii) $\varphi \in X \Rightarrow (\neg\varphi) \in X$,
(iv) $\varphi \in X \Rightarrow ((\forall x_i)\varphi), ((\exists x_i)\varphi) \in X$.

$FORM$ é o nosso *conjunto de fórmulas*. Introduzimos $t_1 = t_2$ separadamente, mas poderíamos tê-la admitido como um caso particular da primeira cláusula. Se conveniente, não trataremos a igualdade separadamente. As fórmulas introduzidas em (i) são chamadas *átomos*. Note que (i) inclui o caso dos símbolos de predicado 0-ários, convenientemente chamados de símbolos proposicionais.

Um símbolo proposicional é interpretado como uma relação 0-ária, i.e. como 0 ou 1 (cf. 2.2.2). Isso está de acordo com a prática da lógica proposicional de interpretar proposições como verdadeiro ou falso. Para os nossos objetivos no momento, proposições são objetos de luxo. Quando se está lidando com situações matemáticas concretas (e.g. grupos ou conjuntos parcialmente ordenados) não se tem razão para introduzir proposições (coisas com um valor-verdade fixo). Entretanto, proposições são convenientes (e importantes) no contexto da lógica de valores booleanos ou da lógica de valores sobre uma álgebra de Heyting, e em considerações sintáticas.

Admitiremos, no entanto, a existência de uma proposição especial: $\perp$, o símbolo para a proposição falsa (cf. 1.2).

Os conectivos lógicos têm o que se poderia chamar de 'domínio de ação', e.g. em $\varphi \rightarrow \psi$ o conectivo $\rightarrow$ dá origem à nova fórmula $\varphi \rightarrow \psi$ a partir das fórmulas $\varphi$ e $\psi$, e portanto $\rightarrow$ age sobre $\varphi$, $\psi$ e todas as partes dessas fórmulas. Para os conectivos proposicionais isso não é muito interessante, mas o é para os quantificadores (e operadores quaisquer que ligam variáveis). A noção a que nos referimos é chamada de *escopo*. Portanto em $((\forall x)\varphi)$ e $((\exists x)\varphi)$, $\varphi$ é o *escopo do quantificador*. Por uma simples verificação do casamento dos parênteses pode-se efetivamente encontrar o escopo de um quantificador. Se uma variável, termo ou fórmula ocorre em $\varphi$, dizemos que ela está no escopo do quantificador em $\forall x\varphi$ ou $\exists x\varphi$.

Tal qual no caso de $PROP$, temos princípios de indução para $TERM$ e $FORM$.

**Lema 2.3.3** *Seja $A(t)$ uma propriedade de termos. Se $A(t)$ se verifica quando $t$ é uma variável ou uma constante, e se $A(t_1), A(t_2), \ldots \Rightarrow A(f(t_1, \ldots, t_n))$, para todos os símbolos de função $f$, então $A(t)$ se verifica para todo $t \in TERM$.*

*Demonstração.* Cf. 1.1.3. □

**Lema 2.3.4** *Seja $A(\varphi)$ uma propriedade de fórmulas. Se*
(i) $A(\varphi)$ *para* $\varphi$ *atômica,*
(ii) $A(\varphi), A(\psi) \Rightarrow A(\varphi \square \psi)$,
(iii) $A(\varphi) \Rightarrow A(\neg\varphi)$,
(iv) $A(\varphi) \Rightarrow A((\forall x_i)\varphi), A((\exists x_i)\varphi)$ *para todo $i$, então $A(\varphi)$ se verifica para toda $\varphi \in FORM$.*

*Demonstração.* Cf. 1.1.3. □

Introduziremos imediatamente um número de abreviações. Em primeiro lugar adotamos as convenções de parentização da lógica proposicional. Além do mais omitimos os parênteses mais externos e os parênteses em torno de $\forall x$ e $\exists x$, sempre que possível. Estamos de acordo que os quantificadores têm prioridade sobre conectivos binários. Além disso juntamos cadeias de quantificadores, e.g. $\forall x_1 x_2 \exists x_3 x_4 \varphi$ designa $\forall x_1 \forall x_2 \exists x_3 \exists x_4 \varphi$. Para maior facilidade de leitura das fórmulas vamos algumas vezes separar o quantificador da fórmula por meio de um ponto: $\forall x \cdot \varphi$. Assumiremos também que $n$ em $f(t_1, \ldots, t_n)$, $P(t_1, \ldots, t_n)$ sempre indica o número correto de argumentos.

*Uma palavra de advertência*: o uso de = pode confundir um leitor desavisado. O símbolo '=' é usado na linguagem $L$, onde ele é um objeto sintático propriamente dito. Ele ocorre em fórmulas tais como $x_0 = x_7$, mas ele também ocorre na meta-linguagem, e.g. na forma $x = y$, que deve ser lido como "$x$ e $y$ são a mesma variável". Entretanto, o símbolo da identidade em $x = y$ é um meta-átomo, que pode ser convertido em um átomo propriamente dito substituindo-se símbolos genuínos de variáveis por $x$ e $y$. Alguns autores usam $\equiv$ para "sintaticamente idênticos", como em "$x$ e $y$ são a mesma variável". Optaremos por "=" para a igualdade em estruturas (conjuntos), e por "$\doteq$" para o símbolo de predicados correspondente à identidade na linguagem. Usaremos $\doteq$ algumas vezes, mas preferimos permanecer com um simples "=" confiando que o leitor estará atento.

**Exemplo 2.3.5** Exemplo de uma linguagem de tipo $\langle 2; 2, 1; 1 \rangle$.

| | |
|---|---|
| símbolos de predicado: | $M$, $\doteq$ |
| símbolos de função: | $p$, $i$ |
| símbolos de constante: | $\overline{e}$ |

Alguns termos: $t_1 := x_0$; $t_2 := p(x_1, x_2)$; $t_3 := p(\overline{e}, \overline{e})$; $t_4 := i(x_7)$; $t_5 := p(i(p(x_2, \overline{e})), i(x_1))$.

Algumas fórmulas:

$$
\begin{aligned}
\varphi_1 &:= x_0 \doteq x_2, \\
\varphi_2 &:= t_3 \doteq t_4, \\
\varphi_3 &:= M(i(x_5), \overline{e}), \\
\varphi_4 &:= (x_0 \doteq x_1 \to x_1 \doteq x_0), \\
\varphi_5 &:= (\forall x_0)(\forall x_1)(x_0 \doteq x_1 \to \neg M(x_0, x_1)), \\
\varphi_6 &:= (\forall x_0)(\exists x_1)(p(x_0, x_1) \doteq \overline{e}), \\
\varphi_7 &:= (\exists x_1)(\neg x_1 \doteq \overline{e} \wedge p(x_1, x_1) \doteq \overline{e}).
\end{aligned}
$$

(Escolhemos uma notação sugestiva; pense na linguagem dos grupos ordenados: $M$ para designar "menor que", $p, i$ para "produto" e "inverso"). Note que a ordem na qual os vários símbolos são listados é importante. Em nosso exemplo $p$ tem 2 argumentos e $i$ tem 1.

Em matemática existem um número de *operações que ligam variáveis*, tais como somatório, integração, abstração: considere, por exemplo, integração, em $\int_0^1 \sin x dx$ a variável tem um papel pouco usual para uma variável. Pois $x$ não pode "variar"; não podemos (sem acaber escrever besteira) substituir $x$ por qualquer número que desejemos. Na integral a variável $x$ é reduzida a uma marca. Dizemos que uma variável $x$ é ligada pelo símbolo da integração. De forma análoga distinguimos em lógica entre variáveis *livres* e variáveis *ligadas*.

Ao definir várias noções sintáticas novamente faremos livremente uso do princípio da *definição por recursão* (cf. 1.1.6). A justificativa é imediata: o valor de um termo (ou fórmula) é unicamente determinado pelos valores de suas partes. Isso nos permite encontrar o valor de $H(t)$ em um número finito de passos.

**Definição por Recursão sobre** $TERM$**:** Seja $H_0 : Var \cup Const \to A$ (i.e. o mapeamento $H_0$ é definido sobre variáveis e constantes), $H_i : A^{a_i} \to A$, então existe um único mapeamento $H : TERM \to A$ tal que

$$\begin{cases} H(t) = H_0(t) \text{ para } t \text{ uma variável ou uma constante,} \\ H(f_i(t_1, \ldots, t_{a_i})) = H_i(H(t_1), \ldots H(t_{a_i})). \end{cases}$$

**Definição por Recursão sobre** $FORM$**:**

$$\begin{array}{lll} \text{Seja} & H_{at} : At \to A & \text{(i.e. } H_{at} \text{ é definido sobre átomos),} \\ & H_\Box : A^2 \to A, & (\Box \in \{\vee, \wedge, \to, \leftrightarrow\}), \\ & H_\neg : A \to A, & \\ & H_\forall : A \times N \to A, & \\ & H_\exists : A \times N \to A. & \end{array}$$

então existe um único mapeamento $H : FORM \to A$ tal que

$$\begin{cases} H(\varphi) & = & H_{at}(\varphi) \text{ para } \varphi \text{ atômica,} \\ H(\varphi \Box \psi) & = & H_\Box(H(\varphi), H(\psi)), \\ H(\neg\varphi) & = & H_\neg(H(\varphi)), \\ H(\forall x_i \varphi) & = & H_\forall(H(\varphi), i), \\ H(\exists x_i \varphi) & = & H_\exists(H(\varphi), i). \end{cases}$$

**Definição 2.3.6** O conjunto $VL(t)$ de variáveis livres de $t$ é definido por

$$\begin{array}{llll} \text{(i)} & VL(x_i) & := & \{x_i\}, \\ & VL(\overline{c}_i) & := & \emptyset \\ \text{(ii)} & VL(f(t_1, \ldots, t_n)) & := & VL(t_1) \cup \ldots \cup VL(t_n). \end{array}$$

*Observação.* Para evitar notação sobrecarregada omitiremos os índices e assumiremos tacitamente que o número de argumentos está correto. O leitor pode facilmente acrescentar os detalhes corretos, caso deseje.

**Definição 2.3.7** O conjunto $VL(\varphi)$ de variáveis livres de $\varphi$ é definido por

$$\begin{array}{llll} \text{(i)} & VL(P(t_1, \ldots, t_p)) & := & VL(t_1) \cup \ldots \cup VL(t_p), \\ & VL(t_1 = t_2) & := & VL(t_1) \cup VL(t_2), \\ & VL(\bot) = VL(P) & := & \emptyset \text{ para } P \text{ um símbolo proposicional,} \\ \text{(ii)} & VL(\varphi \Box \psi) & := & VL(\varphi) \cup VL(\psi), \\ & VL(\neg\varphi) & := & VL(\varphi), \\ \text{(iii)} & VL(\forall x_i \varphi) = VL(\exists x_i \varphi) & := & VL(\varphi) - \{x_i\}. \end{array}$$

**Definição 2.3.8** $t$ ou $\varphi$ são chamados de *fechados* se $VL(t) = \emptyset$, respectivamente $VL(\varphi) = \emptyset$. Uma fórmula fechada é também chamada de *sentença*. Uma fórmula sem quantificadores é chamada de *aberta*. $TERM_c$ designa o conjunto de termos fechados; $SENT$ designa o conjunto de sentenças.

A definição do conjunto $VLig(\varphi)$ de *variáveis ligadas* de $\varphi$ é deixada ao leitor.

*Continuação do Exemplo* 2.3.5.
$VL(t_2) = \{x_1, x_2\}$; $VL(t_3) = \emptyset$; $VL(\varphi_2) = VL(t_3) \cup VL(t_4) = \{x_7\}$; $VL(\varphi_7) = \emptyset$; $VLig(\varphi_4) = \emptyset$; $VLig(\varphi_6) = \{x_0, x_1\}$. $\varphi_5, \varphi_6, \varphi_7$ são sentenças.

*Advertência.* O conjunto $VL(\varphi) \cap VLig(\varphi)$ não é necessariamente vazio; em outras palavras, a mesma variável pode ocorrer livre *e* ligada. Para lidar com tais situações pode-se considerar ocorrências livres (respectivamente ligadas) de variáveis. Quando necessário faremos informalmente uso de ocorrências de variáveis.

*Exemplo.* $\forall x_1(x_1 = x_2) \to P(x_1)$ contém $x_1$ livre e ligada, pois a ocorrência de $x_1$ em $P(x_1)$ não está no escopo do quantificador.

No cálculo de predicados temos operadores de substituição para termos e para fórmulas.

**Definição 2.3.9** Sejam $s$ e $t$ termos, então $s[t/x]$ é definido da seguinte forma:

$$
\begin{array}{lll}
\text{(i)} & y[t/x] & := \begin{cases} y & \text{se } y \not\equiv x, \\ t & \text{se } y \equiv x, \end{cases} \\
 & c[t/x] & := c, \\
\text{(ii)} & f(t_1, \dots, t_p)[t/x] & := f(t_1[t/x], \dots, t_p[t/x]).
\end{array}
$$

Note que na cláusula (i) $y \equiv x$ significa "$x$ e $y$ são a mesma variável".

**Definição 2.3.10** $\varphi[t/x]$ é definido da seguinte maneira:

$$
\begin{array}{lll}
\text{(i)} & \bot[t/x] & := \bot, \\
 & P[t/x] & := P \text{ para proposições } P, \\
 & P(t_1, \dots, t_p)[t/x] & := P(t_1[t/x], \dots, t_p[t/x]), \\
 & (t_1 = t_2)[t/x] & := t_1[t/x] = t_2[t/x], \\
\text{(ii)} & (\varphi \Box \psi)[t/x] & := \varphi[t/x] \Box \psi[t/x], \\
 & (\neg\varphi)[t/x] & := \neg\varphi[t/x], \\
\text{(iii)} & (\forall y\, \varphi)[t/x] & := \begin{cases} \forall y\, \varphi[t/x] & \text{se } x \not\equiv y, \\ \forall y\, \varphi & \text{se } x \equiv y, \end{cases} \\
 & (\exists y\, \varphi)[t/x] & := \begin{cases} \exists y\, \varphi[t/x] & \text{se } x \not\equiv y, \\ \exists y\, \varphi & \text{se } x \equiv y. \end{cases}
\end{array}
$$

A substituição de fórmulas é definida como no caso de proposições, e por conveniência usamos '\$' como um símbolo para designar o símbolo proposicional (ou seja, um símbolo de predicado 0-ário) que age como um 'guardador de lugar'.

**Definição 2.3.11** $\sigma[\varphi/\$]$ é definido da seguinte forma:

$$\begin{array}{lll} \text{(i)} & \sigma[\varphi/\$] & := \left\{\begin{array}{ll}\sigma & \text{se } \sigma \not\equiv \$ \\ \varphi & \text{se } \sigma \equiv \$\end{array}\right. \text{ para } \sigma \text{ atômica,} \\ \text{(ii)} & (\sigma_1 \Box \sigma_2)[\varphi/\$] & := \sigma_1[\varphi/\$] \Box \sigma_2[\varphi/\$], \\ & (\neg\sigma_1)[\varphi/\$] & := \neg\sigma_1[\varphi/\$], \\ & (\forall y\, \sigma)[\varphi/\$] & := \forall y.\sigma[\varphi/\$], \\ & (\exists y\, \sigma)[\varphi/\$] & := \exists y.\sigma[\varphi/\$]. \end{array}$$

*Continuação do Exemplo 2.3.5.*

$$\begin{array}{lll} t_4[t_2/x_1] & = & i(x_7); \\ t_4[t_2/x_7] & = & i(p(x_1, x_2)); \\ t_5[x_2/x_1] & = & p(i(p(x_2, \overline{e}), i(x_2)), \\ \varphi_1[t_3/x_0] & = & p(\overline{e}, \overline{e}) \doteq x_2; \\ \varphi_5[t_3/x_0] & = & \varphi_5. \end{array}$$

Algumas vezes faremos *substituições simultâneas*, cuja definição é uma pequena modificação das definições 2.3.9, 2.3.10, 2.3.11. O leitor é convidado a escrever as definições formais. Escrevemos $t[t_1, \ldots, t_n/y_1, \ldots, y_n]$ para designar a substituição de $y_1, \ldots, y_n$ por $t_1, \ldots, t_n$ simultaneamente. (Igualmente para $\varphi$.)

Note que uma substituição simultânea não é o mesmo que sua correspondente substituição repetida.

*Exemplo.*

$$\begin{array}{llllll} & (x_0 \doteq x_1)[x_1, x_0/x_0, x_1] & = & (x_1 \doteq x_0), & & \\ \text{mas} & ((x_0 \doteq x_1)[x_1/x_0])[x_0/x_1] & = & (x_1 \doteq x_1)[x_0/x_1] & = & (x_0 \doteq x_0). \end{array}$$

A clásula dos quantificadores na definição 2.3.10 proíbe a substituição de variáveis ligadas. Existe, no entanto, mais um caso em que desejamos usar uma proibição: uma substituição na qual alguma variável torna-se ligada após a substituição. Daremos um exemplo de tal substituição; a razão pela qual proibimos que a substituição seja efetuada é que ela pode modificar o valor-verdade de uma maneira absurda. Nesse momento não temos uma definição de verdade, portanto o argumento é puramente heurístico.

*Exemplo.* $\exists x(y < x)[x/y] \quad = \quad \exists x(x < x)$.

Note que a fórmula do lado direito é falsa em uma estrutura ordenada, enquanto que $\exists x(y < x)$ pode muito bem ser verdadeira. Vamos tornar nossa restrição mais precisa:

**Definição 2.3.12** *$t$ é livre para $x$ em $\varphi$* se

(i) $\varphi$ é atômica,

(ii) $\varphi := \varphi_1 \Box \varphi_2$ (ou $\varphi := \neg\varphi_1$) e $t$ é livre para $x$ em $\varphi_1$ e $\varphi_2$ (resp. $\varphi_1$),

(iii) $\varphi := \exists y\, \psi$, ou $\varphi := \forall y\, \psi$, e $y \notin VL(t)$ e $t$ é livre para $x$ em $\psi$, onde $x \neq y$.

*Exemplos.*
1. $x_2$ é livre para $x_0$ em $\exists x_3\, P(x_0, x_3)$,
2. $f(x_0, x_1)$ não é livre para $x_0$ em $\exists x_1\, P(x_0, x_3)$,
3. $x_5$ é livre para $x_1$ em $P(x_1, x_3) \to \exists x_1\, Q(x_1, x_2)$.

Para todos os propósitos práticos o uso de "$t$ é livre para $x$ em $\varphi$" consiste do fato de que as variáveis (livres) de $t$ não vão se tornar ligadas após a substituição em $\varphi$.

**Lema 2.3.13** *$t$ é livre para $x$ em $\varphi \Leftrightarrow$ as variáveis de $t$ em $\varphi[t/x]$ não são ligadas por um quantificador.*

*Demonstração.* Indução sobre $\varphi$.

– Para $\varphi$ atômica o lema é evidente.

– $\varphi = \varphi_1 \Box \varphi_2$. $t$ é livre para $x$ em $\varphi \overset{def}{\Leftrightarrow}$ $t$ é livre para $x$ em $\varphi_1$ e $t$ é livre para $x$ em $\varphi_2 \overset{h.i.}{\Leftrightarrow}$ as variáveis de $t$ em $\varphi_1[t/x]$ não são ligadas por um quantificador e as variáveis de $t$ em $\varphi_2[t/x]$ não são ligadas por um quantificador $\Leftrightarrow$ as variáveis de $t$ em $(\varphi_1 \Box \varphi_2)[t/x]$ não são ligadas por um quantificador.

– $\varphi = \neg\varphi_1$, semelhante.

– $\varphi = \forall y\, \psi$. $t$ é livre para $x$ em $\varphi \overset{def}{\Leftrightarrow} y \notin VL(t)$ e $t$ é livre para $x$ em $\psi \overset{h.i.}{\Leftrightarrow}$ as variáveis de $t$ não estão no escopo de $\forall y$ e as variáveis de $t$ em $\psi[t/x]$ não são ligadas por um (outro) quantificador $\Leftrightarrow$ as variáveis de $t$ em $\varphi[t/x]$ não são ligadas por um quantificador. $\Box$

Existe uma definição análoga e um lema análogo para a substituição de fórmulas.

**Definição 2.3.14** $\varphi$ é livre para \$ em $\sigma$ se:
(i) $\sigma$ é atômica,
(ii) $\sigma := \sigma_1 \Box \sigma_2$ (ou $\neg\sigma_1$) e $\varphi$ é livre para \$ em $\sigma_1$ e em $\sigma_2$ (ou em $\sigma_1$),
(iii) $\sigma := \exists y\, \tau$ (ou $\forall y\, \tau$) e $y \notin VL(\varphi)$ e $\varphi$ é livre para \$ em $\tau$.

**Lema 2.3.15** *$\varphi$ é livre para \$ em $\sigma \Leftrightarrow$ as variáveis livres de $\varphi$ não são ligadas por um quantificador em $\sigma[\varphi/\$]$.*

*Demonstração.* Tal qual a demonstração do Lema 2.3.13. $\Box$

A partir de agora assumimos tacitamente que todas as nossas substituições são "livres para". Por conveniência introduzimos uma notação informal que simplifica a leitura e a escrita:

*Notação.* De modo a simplificar a notação de substituição e procurando permanecer de acordo com uma tradição antiga e sugestiva escreveremos (meta-)expressões como $\varphi(x, y, z)$, $\psi(x, x)$, etc. Isso nem significa que as variáveis listadas ocorrem livre, nem que nenhuma outra ocorre livre. É simplesmente uma maneira conveniente de lidar com substituições informalmente: $\varphi(t)$ é o resultado de se substituir $x$ por $t$ em $\varphi(x)$; $\varphi(t)$ é chamada de *instância de substituição* de $\varphi(x)$.

Usamos as linguagens introduzidas acima para descrever estruturas, ou classes de estruturas de um dado tipo. Os símbolos de predicado, símbolos de função e os símbolos de constante agem como nomes para várias relações, operações e constantes. Ao descrever uma estrutura é de grande ajuda ser capaz de se referir a todos os elementos de $|\mathrm{A}|$, i.e. dispor de *nomes* para todos os elementos (embora que apenas como um dispositivo auxiliar). Por conseguinte introduzimos:

**Definição 2.3.16** A *linguagem estendida*, $L(\mathrm{A})$ de A é obtida a partir da linguagem $L$, do tipo de A, adicionando-se símbolos de constante para todos os elementos de A. Usamos $\overline{a}$ para fazer referência ao símbolo de constante correspondente ao elemento $a \in |\mathrm{A}|$.

*Exemplo.* Considere a linguagem $L$ dos grupos; então $L(\mathrm{A})$, para A o grupo aditivo dos inteiros, tem símbolos de constante (extras) $\overline{0}$, $\overline{1}$, ..., $\overline{-1}$, $\overline{-2}$, $\overline{-3}$, .... Observe que dessa maneira 0 tem dois nomes: o nome antigo e um dos nomes novos. Isso não é problema, pois por que razão algum objeto não deveria ter mais que um nome?

**Exercícios**

1. Escreva um alfabeto para as linguagens dos tipos dados no Exercício 1 da seção 2.2.

2. Escreva cinco termos da linguagem do Exercício 1 (iii), (viii). Escreva duas fórmulas atômicas da linguagem do Exercício 1 (vii) e dois átomos fechados da linguagem do Exercício 1 (iii), (vi).

3. Escreva um alfabeto para linguagens de tipos $\langle 3; 1, 1, 2; 0\rangle$, $\langle -; 2; 0\rangle$ e $\langle 1; -; 3\rangle$.

4. Verifique quais termos são livres nos seguintes casos, e realize a operação de substituição:

   (a) $x$ para $x$ em $x = x$,
   (b) $y$ para $x$ em $x = x$,
   (c) $x + y$ para $y$ em $z = \overline{0}$
   (d) $\overline{0} + y$ para $y$ em $\exists x(y = x)$,
   (e) $x + y$ para $z$ em $\exists w(w + x = \overline{0})$,
   (f) $x + w$ para $z$ em $\forall w(x + z = \overline{0})$,
   (g) $x + y$ para $z$ em $\forall w(x + z = \overline{0}) \wedge \exists y(z = x)$,
   (h) $x + y$ para $z$ em $\forall u(u = v) \to \forall z(z = y)$.

## 2.4 Semântica

A arte de interpretar enunciados (matemáticos) pressupõe uma rígida separação entre "linguagem" e o "universo" matemático de entidades. Os objetos da linguagem são símbolos, ou cadeias de símbolos, as entidades da matemática são números, conjuntos, funções, triângulos, etc. É uma questão para a filosofia da matemática refletir sobre o universo da matemática; aqui simplesmente aceitaremos o que nos é dado. Nossas necessidades com relação ao universo matemático são, no momento, bem modestas. Igualmente, nossos desidérios com respeito à linguagem são modestos. Apenas supomos que existe um suprimento ilimitado de símbolos.

A idéia por trás da semântica da lógica de predicados é muito simples. Seguindo Tarski, assumimos que um enunciado $\sigma$ é verdadeiro em uma estrutura, se é de fato o caso que $\sigma$ se aplica (a sentença "A neve é branca" é verdadeira se a neve é de fato branca). Um exemplo matemático: "$\overline{2}+\overline{2}=\overline{4}$" é verdadeiro na estrutura dos números naturais (com adição) se $2+2=4$ (i.e. se a adição dos *números* 2 e 2 resulta no *número* 4.) Interpretação é a arte de relacionar objetos sintáticos (cadeias de símbolos) e estados de coisas "na realidade".

Vamos começar dando um exemplo de uma interpretação em um caso simples. Consideramos a estrutura $\mathrm{A} = (\mathbb{Z}, <, +, -, 0)$, i.e. o grupo ordenado dos inteiros.

A linguagem tem no seu alfabeto:

| | |
|---|---|
| *símbolos de predicado* | : $\doteq$, $L$ |
| *símbolos de função* | : $P$, $M$ |
| *símbolos de constante* | : $\overline{0}$ |

$L(\mathrm{A})$ tem, além de tudo isso, símbolos de constante $\overline{m}$ para todo $m \in \mathbb{Z}$. Primeiro interpretamos os termos fechados de $L(\mathrm{A})$; a interpretação $t^{\mathrm{A}}$ de um termo $t$ é um elemento de $\mathbb{Z}$.

| $t$ | $t^{\mathrm{A}}$ |
|---|---|
| $\overline{m}$ | $m$ |
| $S(t_1, t_2)$ | $t_1^{\mathrm{A}} + t_2^{\mathrm{A}}$ |
| $M(t)$ | $-t^{\mathrm{A}}$ |

Grosso modo, interpretamos $\overline{m}$ como "seu número", $S$ como *soma*, $M$ como *menos*. Note que interpretamos apenas termos fechados. Isso faz sentido, pois como se deveria atribuir um inteiro definitivo a $x$?

A seguir interpretamos *sentenças* de $L(\mathrm{A})$ atribuindo um dos valores 0 ou 1. No que concerne aos conectivos proposicionais, seguimos a semântica para a lógica proposicional.

$$
\begin{array}{lcl}
v(\bot) & = & 0, \\
v(t \doteq s) & = & \begin{cases} 1 & \text{se } t^{\mathrm{A}} = s^{\mathrm{A}} \\ 0 & \text{caso contrário,} \end{cases} \\
v(L(t,s)) & = & \begin{cases} 1 & \text{se } t^{\mathrm{A}} < s^{\mathrm{A}} \\ 0 & \text{caso contrário,} \end{cases} \\
\begin{array}{c} v(\varphi \Box \psi) \\ v(\neg\varphi) \end{array} & & \text{tal qual na Definição 1.2.1} \\
v(\forall x \varphi) & = & \min\{v(\varphi[\overline{n}/x]) \mid n \in \mathbb{Z}\} \\
v(\exists x \varphi) & = & \max\{v(\varphi[\overline{n}/x]) \mid n \in \mathbb{Z}\}
\end{array}
$$

Algumas observações são necessárias.

1. Na realidade definimos uma função $v$ por recursão sobre $\varphi$.

2. A valoração de uma fórmula universalmente quantificada é obtida tomando-se o mínimo de todas as valorações das instâncias individuais, i.e. o valor é 1 (verdadeiro) sse todas as instâncias têm o valor 1. Nesse sentido $\forall$ é uma generalização de $\wedge$. Igualmente $\exists$ é uma generalização de $\vee$.

3. $v$ é determinado de forma unívoca por A, portanto $v_{\mathrm{A}}$ seria uma notação mais apropriada. Por conveniência permaneceremos com a notação simplificada $v$.

4. Tal qual na semântica da lógica proposicional, escreveremos $[\![\varphi]\!]_{\mathrm{A}}$ para designar $v_{\mathrm{A}}(\varphi)$, e quando não existir possibilidade de haver confusão omitiremos o índice A.

5. Seria tentador tornar nossa notação realmente uniforme escrevendo $[\![t]\!]_{\mathrm{A}}$ no lugar de $t^{\mathrm{A}}$. Entretanto, manteremos ambas as notações e usaremos a que for mais legível. A notação em que aparece o expoente tem a desvantagem de que requer mais parênteses, mas a notação $[\![\ ]\!]$ não melhora a legibilidade.

*Exemplos.*

1. $(S(S(\overline{2},\overline{3}),M(\overline{7})))^{\mathrm{A}} = S(\overline{2},\overline{3}) + M(\overline{7})^{\mathrm{A}}) = \overline{(\overline{2}^{\mathrm{A}} + \overline{3}^{\mathrm{A}}) + (-\overline{7}^{\mathrm{A}})} = 2 + 3 + (-7) = -2$,

2. $[\![\overline{2} \doteq \overline{1}]\!] = 0$, pois $2 \neq -1$,

3. $[\![\overline{0} \doteq \overline{1} \to L(\overline{25},\overline{10})]\!] = 1$, pois $[\![\overline{0} \doteq \overline{1}]\!] = 0$ e $[\![L(\overline{25},\overline{10})]\!] = 0$; pela interpretação da implicação o valor é 1,

4. $[\![\forall x \exists y(L(x,y)) = \min_n(\max_m [\![L(\overline{n},\overline{m})]\!])$

   $[\![L(\overline{n},\overline{m})]\!] = 1$ para $m > n$, logo para um $n$ fixo, $\max_m([\![L(\overline{n},\overline{m})]\!]) = 1$, e portanto $\min_n \max_m [\![L(\overline{n},\overline{m})]\!] = 1$.

Vamos agora apresentar uma definição de interpretação para o caso geral. Considere $\mathrm{A} = \langle A, R_1, \ldots, R_n, F_1, \ldots, F_m, \{c_i \mid i \in I\}\rangle$ de um dado tipo de similaridade $\langle r_1, \ldots, r_n; a_1, \ldots, a_m; |I|\rangle$.

A linguagem correspondente tem símbolos de predicado $\overline{R}_1, \ldots, \overline{R}_n$, símbolos de função $\overline{F}_1, \ldots, \overline{F}_m$ e símbolos de constante $\overline{c}_i$. $L(\mathrm{A})$, além do mais, tem símbolos de constante $\overline{a}$ para todo $a \in |\mathrm{A}|$.

**Definição 2.4.1** Uma interpretação dos termos fechados de $L(\mathrm{A})$ em A é um mapeamento $(\cdot)^{\mathrm{A}} : TERM_c \to |\mathrm{A}|$ satisfazendo:

$$\begin{array}{lll} (i) & \overline{c}_i^{\mathrm{A}} & = c_i, \\ & \overline{a}^{\mathrm{A}} & = a, \\ (ii) & (\overline{F}_i(t_1,\ldots,t_p))^{\mathrm{A}} & = F_i(t_1^{\mathrm{A}},\ldots,t_p^{\mathrm{A}}),\ \text{onde } p = a_i. \end{array}$$

Também escreveremos $[\![t]\!]_{\mathrm{A}}$ para designar $t^{\mathrm{A}}$. A escolha é uma questão de conveniência ou convenção.

**Definição 2.4.2** Uma interpretação das sentenças $\varphi$ de $L(\mathrm{A})$ em A é um mapeamento $(\cdot)^{\mathrm{A}} : SENT \to \{0,1\}$, satisfazendo:

$$
\begin{array}{lll}
(i) & [\![\bot]\!]_{\mathrm{A}} & := 0, \\
 & [\![\overline{R}]\!]_{\mathrm{A}} & := R \text{ i.e. } 0 \text{ ou } 1). \\
(ii) & [\![\overline{R}_i(t_1,\ldots,t_p)]\!]_{\mathrm{A}} & := \begin{cases} 1 & \text{se } \langle t_1^{\mathrm{A}},\ldots,t_p^{\mathrm{A}}\rangle \in R_i, \text{ onde } p = r_i, \\ 0 & \text{caso contrário.} \end{cases} \\
 & [\![t_1 \doteq t_2]\!]_{\mathrm{A}} & := \begin{cases} 1 & \text{se } t_1^{\mathrm{A}} = t_2^{\mathrm{A}} \\ 0 & \text{caso contrário.} \end{cases} \\
(iii) & [\![\varphi \wedge \psi]\!]_{\mathrm{A}} & := \min([\![\varphi]\!]_{\mathrm{A}}, [\![\psi]\!]_{\mathrm{A}}), \\
 & [\![\varphi \vee \psi]\!]_{\mathrm{A}} & := \max([\![\varphi]\!]_{\mathrm{A}}, [\![\psi]\!]_{\mathrm{A}}), \\
 & [\![\varphi \to \psi]\!]_{\mathrm{A}} & := \max(1 - [\![\varphi]\!]_{\mathrm{A}}, [\![\psi]\!]_{\mathrm{A}}), \\
 & [\![\varphi \leftrightarrow \psi]\!]_{\mathrm{A}} & := 1 - |[\![\varphi]\!]_{\mathrm{A}} - [\![\psi]\!]_{\mathrm{A}}|, \\
 & [\![\neg\varphi]\!]_{\mathrm{A}} & := 1 - [\![\varphi]\!]_{\mathrm{A}}. \\
(iv) & [\![\forall x\varphi]\!]_{\mathrm{A}} & := \min\{[\![\varphi[\overline{a}/x]]\!]_{\mathrm{A}} \mid a \in |\mathrm{A}|\}, \\
 & [\![\exists x\varphi]\!]_{\mathrm{A}} & := \max\{[\![\varphi[\overline{a}/x]]\!]_{\mathrm{A}} \mid a \in |\mathrm{A}|\}.
\end{array}
$$

*Convenção.* Daqui por diante assumiremos que todas as estruturas e todas as linguagens têm tipos de similaridade apropriados, de modo que não temos que especificar os tipos toda vez.

Na lógica de predicados existe uma alternativa conveniente e popular para a notação envolvendo o símbolo $v$ de valoração:

A $\models \varphi$ denota $[\![\varphi]\!]_{\mathrm{A}} = 1$. Dizemos que "$\varphi$ é verdadeira, válida, em A" se A $\models \varphi$. A relação $\models$ é chamada de *relação de satisfação*.
Note que a mesma notação é disponível em lógica proposicional — lá o papel de A é exercido pela valoração, por isso poder-se-ia muito bem escrever $v \models \varphi$ no lugar de $[\![\varphi]\!]_v = 1$.

Até agora definimos a noção de verdade apenas para sentenças de $L(\mathrm{A})$. De modo a estender $\models$ para fórmulas arbitrárias vamos introduzir uma nova notação.

**Definição 2.4.3** Seja $VL(\varphi) = \{z_1,\ldots,z_k\}$, então $Fecho(\varphi) := \forall z_1 \ldots z_k\varphi$ é o *fecho universal* de $\varphi$ (assumimos que a ordem de ocorrência das variáveis $z_i$ tenha sido fixada de alguma forma).

**Definição 2.4.4** (i) A $\models \varphi$ sse A $\models Fecho(\varphi)$,
(ii) $\models \varphi$ sse A $\models \varphi$ para toda A (do tipo apropriado),
(iii) A $\models \Gamma$ sse A $\models \psi$ para toda $\psi \in \Gamma$,
(iv) $\Gamma \models \varphi$ sse (A $\models \Gamma \;\Rightarrow\;$ A $\models \varphi$), onde $\Gamma \cup \{\varphi\}$ consiste de sentenças.

Se A $\models \sigma$, chamamos A de um *modelo* de $\sigma$. Em geral: se A $\models \Gamma$, chamamos A de um *modelo* de $\Gamma$. Dizemos que $\varphi$ é *verdadeira* se $\models \varphi$, $\varphi$ é uma *conseqüência semântica* de $\Gamma$ se $\Gamma \models \varphi$, i.e. $\varphi$ se verifica em cada modelo de $\Gamma$. Note que isso tudo é uma generalização imediata da Definição 1.2.4.

Se $\varphi$ é uma fórmula com variáveis livres, digamos $VL(\varphi) = \{z_1,\ldots,z_k\}$, então dizemos que $\varphi$ é *satisfeita por* $a_1,\ldots,a_k \in |\mathrm{A}|$ se A $\models \varphi[\overline{a}_1,\ldots,\overline{a}_k/z_1,\ldots,z_k]$, $\varphi$ é chamada de *satisfatível em* A se existem $a_1,\ldots,a_k$ tais que $\varphi$ é satisfeita por $a_1,\ldots,a_k$ e $\varphi$ é chamada simplesmente de *satisfatível* se ela é satisfatível em alguma estrutura A. Note que $\varphi$ é satisfatível em A sse A $\models \exists z_1 \ldots z_k\varphi$.

As propriedades da relação de satisfação estão correspondendo, de forma compreensível e conveniente, ao significado intuitivo dos conectivos.

**Lema 2.4.5** *Se nos restringirmos a sentenças, então*

| | |
|---|---|
| $(i)$ | $\mathrm{A} \models \varphi \wedge \psi \;\Leftrightarrow\; \mathrm{A} \models \varphi$ *e* $\mathrm{A} \models \psi$, |
| $(ii)$ | $\mathrm{A} \models \varphi \vee \psi \;\Leftrightarrow\; \mathrm{A} \models \varphi$ *ou* $\mathrm{A} \models \psi$, |
| $(iii)$ | $\mathrm{A} \models \neg\varphi \;\Leftrightarrow\; \mathrm{A} \not\models \varphi$, |
| $(iv)$ | $\mathrm{A} \models \varphi \rightarrow \psi \;\Leftrightarrow\; (\mathrm{A} \models \varphi \;\Rightarrow\; \mathrm{A} \models \psi)$, |
| $(v)$ | $\mathrm{A} \models \varphi \leftrightarrow \psi \;\Leftrightarrow\; (\mathrm{A} \models \varphi \;\Leftrightarrow\; \mathrm{A} \models \psi)$, |
| $(vi)$ | $\mathrm{A} \models \forall x\varphi \;\Leftrightarrow\; \mathrm{A} \models \varphi[\overline{a}/x]$, *para todo* $a \in \lvert\mathrm{A}\rvert$, |
| $(vii)$ | $\mathrm{A} \models \exists x\varphi \;\Leftrightarrow\; \mathrm{A} \models \varphi[\overline{a}/x]$, *para algum* $a \in \lvert\mathrm{A}\rvert$, |

*Demonstração.* Imediata da Definição 2.4.2. Vamos fazer dois casos.

(iv) $\mathrm{A} \models \varphi \rightarrow \psi \;\Leftrightarrow\; [\![\varphi \rightarrow \psi]\!]_{\mathrm{A}} = \max(1 - [\![\varphi]\!]_{\mathrm{A}}, [\![\psi]\!]_{\mathrm{A}}) = 1$. Suponha que $\mathrm{A} \models \varphi$, i.e. $[\![\varphi]\!]_{\mathrm{A}} = 1$, então claramente $[\![\psi]\!]_{\mathrm{A}} = 1$, ou $\mathrm{A} \models \psi$.

Reciprocamente, suponha que $\mathrm{A} \models \varphi \;\Leftrightarrow\; \mathrm{A} \models \psi$, e suponha que $\mathrm{A} \not\models \varphi \rightarrow \psi$, então $[\![\varphi \rightarrow \psi]\!]_{\mathrm{A}} = \max(1 - [\![\varphi]\!]_{\mathrm{A}}) = 0$. Logo, $[\![\psi]\!]_{\mathrm{A}} = 0$ e $[\![\varphi]\!]_{\mathrm{A}} = 1$. Contradição.

(vii) $\mathrm{A} \models \exists x\varphi(x) \;\Leftrightarrow\; \max\{[\![\varphi(\overline{a})]\!]_{\mathrm{A}} \mid a \in \lvert\mathrm{A}\rvert\} = 1 \;\Leftrightarrow$ existe um $a \in \lvert\mathrm{A}\rvert$ tal que $[\![\varphi(\overline{a})]\!]_{\mathrm{A}} = 1 \;\Leftrightarrow$ existe um $a \in \lvert\mathrm{A}\rvert$ tal que $\mathrm{A} \models \varphi(\overline{a})$. $\square$

O Lema 2.4.5 nos diz que a interpretação de sentenças em A anda em paralelo à construção das sentenças por meio de conectivos. Em outras palavras, substituímos os conectivos por seus análogos na meta-linguagem e interpretamos os átomos checando as relações na estrutura.

Por exemplo, considere nosso exemplo do grupo aditivo ordenado de inteiros: $\mathrm{A} \models \neg\forall x\exists y(x \doteq S(y, y)) \Leftrightarrow$ não é o caso que para cada número $n$ existe um $m$ tal que $n = 2m \Leftrightarrow$ nem todo número pode ser dividido ao meio em A. Isso é claramente correto, pois tome por exemplo $n = 1$.

Vamos refletir por um momento sobre a valoração de símbolos proposicionais; uma relação 0-ária é um subconjunto de $A^{\emptyset} = \{\emptyset\}$, i.e. ela é $\emptyset$ ou $\{\emptyset\}$ e estas são, quando vistos como ordinais, 0 ou 1. Logo, $[\![\overline{P}]\!]_{\mathrm{A}} = P$, e $P$ é um valor verdade. Isso faz com que nossa definição seja perfeitamente razoável. De fato, mesmo sem estar buscando por um tratamento sistemático, podemos observar que fórmulas correspondem a subconjuntos de $A^k$, onde $k$ é o número de variáveis livres. E.g. seja $VL(\varphi) = \{z_1, \ldots, z_k\}$, então poderíamos por $[\![\varphi]\!]_{\mathrm{A}} = \{\langle a_1, \ldots, a_k\rangle \mid \mathrm{A} \models \varphi(\overline{a}_1, \ldots, \overline{a}_k)\}$ $(= \{\langle \overline{a}_1, \ldots, \overline{a}_n\rangle \mid [\![\varphi(\overline{a}_1, \ldots, \overline{a}_n)]\!]_{\mathrm{A}} = 1\})$, portanto espichando um pouco o significado de $[\![\varphi]\!]_{\mathrm{A}}$. Fica imediatamente claro que a aplicação de quantificadores a $\varphi$ reduz a "dimensão". Por exemplo, $[\![\exists x P(x, y)]\!])_{\mathrm{A}} = \{a \mid \mathrm{A} \models P(\overline{b}, \overline{a})$ para algum $b\}$, que é a projeção de $[\![P(x, y)]\!]_{\mathrm{A}}$ sobre o eixo dos $y$.

## Exercícios

1. Seja $\mathrm{N} = \langle \mathbb{N}, +, \cdot, S, 0\rangle$, e $L$ uma linguagem de tipo $\langle -; 2, 2, 2; 1\rangle$.
   - (i) Dê dois termos distintos $t$ em $L$ tais que $t^{\mathrm{N}} = 5$,
   - (ii) Mostre que para cada número natural $n \in \mathbb{N}$ existe um termo $t$ tal que $t^{\mathrm{N}} = n$,
   - (iii) Mostre que para cada $n \in \mathbb{N}$ existe um número infinito de termos $t$ tais que $t^{\mathrm{A}}$.

2. Seja A a estrutura do exercício 1(v) da seção 2.2. Calcule $(((\overline{1} \rightarrow \overline{0}) \rightarrow \neg\overline{0}) \wedge (\neg\overline{0}) \rightarrow (\overline{1} \rightarrow \overline{0}))^{\mathrm{A}}$, $(\overline{1} \leftarrow \neg(\neg\overline{0} \vee \overline{1}))^{\mathrm{A}}$.

3. Seja A a estrutura do exercício 1(viii), 2.2. Calcule $(|(\overline{\sqrt{3}}) - \overline{-5}|)^{\mathrm{A}}$, $(\overline{1} - (|\overline{(-2)}| - (\overline{5} - \overline{(-2)}))^{\mathrm{A}}$.

4. Que casos do Lema 2.4.5 permanecem corretos se considerarmos fórmulas em geral?

5. Para sentenças $\sigma$ temos $\mathrm{A} \models \sigma$ ou $\mathrm{A} \models \neg\sigma$. Mostre que isso não se verifica para $\varphi$ se $VL(\varphi) \neq \emptyset$. Mostre que nem mesmo para sentenças $\models \sigma$ ou $\models \neg\sigma$ se verifica.

6. Mostre que para termos fechados $t$ e fórmulas $\varphi$ (em $L(\mathrm{A})$:

   $\mathrm{A} \models t = \overline{[\![t]\!]_{\mathrm{A}}}$,

   $\mathrm{A} \models \varphi(t) \leftrightarrow \varphi(\overline{[\![t]\!]_{\mathrm{A}}})$ (Obteremos isso também como um corolário do Teorema da Substituição, 2.5.9).

7. Mostre que $\mathrm{A} \models \varphi \Rightarrow \mathrm{A} \models \psi$ para toda estrutura A, implica $\models \varphi \Rightarrow \models \psi$, mas não o contrário.

## 2.5 Propriedades Simples da Lógica de Predicados

Nossa definição de validade (verdade) foi uma mera extensão da definição baseada em valoração dada para a lógica proposicional. Como conseqüência disso, fórmulas que são instâncias de tautologias são verdadeiras em todas as estruturas A (exercício 1). Portanto podemos copiar muitos resultados das seções 1.2 e 1.3. Usaremos esses resultados com uma simples referência à logica proposicional.

As propriedades específicas concernentes aos quantificadores serão tratadas nesta seção. Primeiro consideramos as generalizações das leis de De Morgan.

**Teorema 2.5.1**
*(i)* $\models \neg\forall x\varphi \leftrightarrow \exists x\neg\varphi$
*(ii)* $\models \neg\exists x\varphi \leftrightarrow \forall x\neg\varphi$
*(iii)* $\models \forall x\varphi \leftrightarrow \neg\exists x\neg\varphi$
*(iv)* $\models \exists x\varphi \leftrightarrow \neg\forall x\neg\varphi$

*Demonstração.* Se não há variáveis livres envolvidas, então as equivalências acima são quase triviais. Vamos fazer um caso geral.

(i) Seja $VL(\forall x\varphi) = \{z_1, \ldots, z_k\}$, então devemos mostrar que

$\mathrm{A} \models \forall z_1 \ldots z_k(\neg\forall x\varphi(x, z_1, \ldots, z_k) \leftrightarrow \exists x\neg\varphi(x, z_1, \ldots, z_k))$, para toda A.

Logo, temos que mostrar que $\mathrm{A} \models \neg\forall x\varphi(x, \overline{a}_1, \ldots, \overline{a}_k)$ para quaisquer $\overline{a}_1, \ldots, \overline{a_k} \in |\mathrm{A}|$. Aplicamos as propriedades da relação $\models$ tal qual listadas no Lema 2.4.5:

$\mathrm{A} \models \neg\forall x\varphi(x, \overline{a}_1, \ldots, \overline{a_k}) \Leftrightarrow \mathrm{A} \not\models forall x\varphi(x, \overline{a}_1, \ldots, \overline{a_k}) \Leftrightarrow$ não é o caso de que para todo $b \in |\mathrm{A}|$ $\mathrm{A} \models \varphi(\overline{b}, \overline{a}_1, \ldots, \overline{a_k}) \Leftrightarrow$ existe um $b \in |\mathrm{A}|$ tal que $\mathrm{A} \models \neg\varphi(\overline{b}, \overline{a}_1, \ldots, \overline{a_k}) \Leftrightarrow \mathrm{A} \models \exists x\neg\varphi(x, \overline{a}_1, \ldots, \overline{a_k})$.

(ii) é tratado analogamente,

(iii) pode ser obtido de (i), (ii),

(iv) pode ser obtido de (i), (ii). □

A ordem em que os quantificadores do mesmo tipo (universal ou existencial) aparecem é irrelevante, e a quantificação sobre uma variável que não ocorre na fórmula pode ser desprezada.

**Teorema 2.5.2**

*(i)* $\models \forall x \forall y \varphi \leftrightarrow \forall y \forall x \varphi$,
*(ii)* $\models \exists x \exists y \varphi \leftrightarrow \exists y \exists x \varphi$,
*(iii)* $\models \forall x \varphi \leftrightarrow \varphi$ *se* $x \notin VL(\varphi)$,
*(iv)* $\models \exists x \varphi \leftrightarrow \varphi$ *se* $x \notin VL(\varphi)$.

*Demonstração.* Deixo ao leitor. □

Já observamos que $\forall$ e $\exists$ são, num certo sentido, generalizações de $\wedge$ e $\vee$. Por conseguinte não é surpresa que $\forall$ (respectivamente $\exists$) distribui sobre $\wedge$ (respectivamente $\vee$). O quantificador $\forall$ (respectivamente $\exists$) distribui sobre $\vee$ (respectivamente $\wedge$) apenas se uma certa condição for satisfeita.

**Teorema 2.5.3**

*(i)* $\models \forall x(\varphi \wedge \psi) \leftrightarrow \forall x \varphi \wedge \forall x \psi$,
*(ii)* $\models \exists x(\varphi \vee \psi) \leftrightarrow \exists x \varphi \vee \forall x \psi$,
*(iii)* $\models \forall x(\varphi(x) \vee \psi) \leftrightarrow \forall x \varphi(x) \vee \psi$ *se* $x \notin VL(\psi)$,
*(iv)* $\models \exists x(\varphi(x) \wedge \psi) \leftrightarrow \exists x \varphi(x) \wedge \psi$ *se* $x \notin VL(\psi)$,

*Demonstração.* (i) e (ii) são imediatos.

(iii) Seja $VL(\forall x(\varphi(x) \vee \psi)) = \{z_1, \ldots, z_k\}$. Temos que mostrar que

$\mathrm{A} \models \forall z_1 \ldots z_k(\forall x(\varphi(x) \vee \psi) \leftrightarrow \forall x \varphi(x) \vee \psi)$ para toda A, portanto mostramos, usando o Lema 2.4.5, que $\mathrm{A} \models \forall x(\varphi(x, \overline{a}_1, \ldots, \overline{a}_k)) \vee \psi(\overline{a}_1, \ldots, \overline{a}_k))$ $\Leftrightarrow$ $\mathrm{A} \models \forall x \varphi(x, \overline{a}_1, \ldots, \overline{a}_k) \vee \psi(\overline{a}_1, \ldots, \overline{a}_k)$ para toda A e todo $\overline{a}_1, \ldots, \overline{a}_k \in |\mathrm{A}|$.

Note que no curso da argumentação $overline bar a_1, \ldots, \overline{a}_k$ permanecem fixos, portanto não precisaremos mencioná-los toda vez.

$\Leftarrow$: $\mathrm{A} \models \forall x \varphi(x, —) \vee \psi(—) \Leftrightarrow \mathrm{A} \models \forall x \varphi(x, —)$ ou $\mathrm{A} \models \psi(—) \Leftrightarrow$ $\mathrm{A} \models \varphi(\overline{b}, —)$ para todo $b$ ou $\mathrm{A} \models \psi(—)$.
Se $\mathrm{A} \models \psi(—)$, então temos também $\mathrm{A} \models \varphi(\overline{b}, —) \vee \psi(—)$ para todo $b$, e portanto $\mathrm{A} \models \forall x \varphi(x, —) \vee \psi(—)$. Se para todo $b$ $\mathrm{A} \models \varphi(\overline{b}, —)$ então $\mathrm{A} \models \varphi(\overline{b}, —) \vee \psi(—)$ para todo $b$, portanto $\mathrm{A} \models \forall x(\varphi(x, —) \vee \psi(—))$.
Em ambos os casos obtemos o resultado desejado.

$\Rightarrow$: Sabemos que para cada $b \in |\mathrm{A}|$ temos que $\mathrm{A} \models \varphi(\overline{b}, —) \vee \psi(—)$.
Se $\mathrm{A} \models \psi(—)$, então temos também que $\mathrm{A} \models \forall x \varphi(x, —) \vee \psi(—)$, e nesse caso terminamos.
Se $\mathrm{A} \not\models \psi(—)$ então temos necessariamente que $\mathrm{A} \models \varphi(\overline{b}, —)$ para todo $b$, logo $\mathrm{A} \models \varphi(x, —)$ e portanto $\mathrm{A} \models \forall x \varphi(x, —) \vee \psi(—)$.

(iv) é semelhante. □

Na demonstração acima ilustramos uma técnica para lidar com as variáveis adicionais $z_1, \ldots, z_k$, que permanecem livres, e que na verdade não desempenham um papel real. Escolhe-se uma seqüência arbitrária de elementos $a_1, \ldots, a_k$ para substituir os $z_i$'s e procura-se mantê-los fixos durante a demonstração. Portanto daqui por diante na maior parte dos casos ignoraremos as variáveis adicionais.

**ADVERTÊNCIA**. $\forall x(\varphi(x) \vee \psi(x)) \to \forall x\varphi(x) \vee \forall x\psi(x)$, e
$\exists x(\varphi(x) \wedge \psi(x)) \to \exists x\varphi(x) \wedge \exists x\psi(x)$ *não* são verdadeiras.

Uma das "tarefas de Cinderela" em lógica é o registro de substituições, o manuseio de substituições iteradas, etc. Vamos enunciar um número de lemas úteis, nenhum deles difícil – trata-se mesmo de trabalho braçal.

Uma palavra de advertência ao leitor: nenhum dessas propriedades sintáticas são difíceis de demonstrar, nem existe grande coisa a ser aprendida dessas demonstrações (a menos que se esteja à procura de objetivos específicos, tal como medir a complexidade de certos predicados); o melhor procedimento é expor as demonstrações diretamente e consultar as provas no livro em caso de emergência.

**Lema 2.5.4** (i) *Sejam $x$ e $y$ variáveis distintas tais que $x \notin VL(r)$, então $(t[s/x])[r/y] = (t[r/y])[s[r/y]/x]$,*

(ii) *sejam $x$ e $y$ variáveis distintas tais que $x \notin VL(s)$, e sejam $t$ e $s$ termos livres para $x$ e $y$ em $\varphi$, então $(\varphi[t/x])[s/y] = (\varphi[s/y])[t[s/y]/x]$,*

(iii) *seja $\psi$ uma fórmula livre para \$ em $\varphi$, e seja $t$ um termo livre para $x$ em $\varphi$ e $\psi$, então $(\varphi[\psi/\$])[t/x] = (\varphi[t/x])[\psi[t/x]/\$]$,*

(iv) *sejam $\varphi, \psi$ fórmulas livres para $\$_1, \$_2$ em $\sigma$, seja $\psi$ uma fórmula livre para $\$_2$ em $\varphi$, e suponha que $\$_1$ não ocorre em $\psi$, então $(\sigma[\varphi/\$_1])[\psi/\$_2] = (\sigma[\psi/\$_2])[\varphi[\psi/\$_2]/\$_1]$.*

*Demonstração.* (i) Indução sobre $t$.

– $t = c$, trivial.

– $t = x$. Então $t[s/x] = s$ e $(t[s/x])[r/y] = s[r/y]$; $(t[r/y])[s[r/y]/x] = x[s[r/y]/x] = s[r/y]$.

– $t = y$. Então $(t[s/x])[r/y] = y[r/y] = r$ e $(t[r/y])[s[r/y]/x] = r[s[r/y]/x] = r$, pois $x \notin VL(r)$.

– $t = z$, onde $z \neq x, y$, trivial.

– $t = f(t_1, \ldots, t_n)$. Então

$$\begin{aligned}
(t[s/x])[r/y] &= (f(t_1[s/x], \ldots, t_n[s/x]))[r/y] \\
&= f((t_1[s/x])[r/y], \ldots, (t_n[s/x])[r/y]) \\
&\overset{h.i.}{=} f((t_1[r/y])[s[r/y]/x], \ldots, (t_n[r/y])[s[r/y]/x]) \\
&= f(t_1[r/y], \ldots, t_n[r/y])[s[r/y]/x] \\
&= (t[r/y])[s[r/y]/x].
\end{aligned}$$

□

Imediatamente obtemos

**Corolário 2.5.5** *(i) Se $z \notin VL(t)$, então $t[\overline{a}/x] = (t[z/x])[\overline{a}/z]$,*
*(ii) Se $z \notin VL(\varphi)$ e $z$ é livre para $x$ em $\varphi$, então $\varphi[\overline{a}/x] = (\varphi[z/x])[\overline{a}/z]$.*

É possível puxar os quantificadores para a frente da fórmula. O truque é bem conhecido em análise: a variável ligada em uma integral pode ser trocada. E.g. $\int xdx + \int \sin ydy = \int xdx + \int \sin xdx = \int (x + \sin x)dx$. Em lógica de predicados temos um fenômeno semelhante.

**Teorema 2.5.6 (Troca de Variáveis Ligadas)** *Se $x, y$ são livres para $z$ em $\varphi$ e $x, y \notin VL(\varphi)$ então*
$\models \exists x\varphi[x/z] \leftrightarrow \exists y\varphi[y/z]$,
$\models \forall x\varphi[x/z] \leftrightarrow \forall y\varphi[y/z]$.

*Demonstração.* Basta considerar $\varphi$ com $VL(\varphi) \subseteq \{z\}$. Temos que mostrar que $\mathfrak{A} \models \exists x\varphi[x/z] \Leftrightarrow \mathfrak{A} \models \exists y\varphi[y/z]$ para qualquer $\mathfrak{A}$.

$\mathfrak{A} \models \exists x\varphi[x/z] \Leftrightarrow \mathfrak{A} \models (\varphi[x/z])[\overline{a}/z]$ para algum $a$
$\Leftrightarrow \mathfrak{A} \models \varphi[\overline{a}/z]$ para algum $a \Leftrightarrow \mathfrak{A} \models (\varphi[y/z])[\overline{a}/y]$ para algum $a \Leftrightarrow \mathfrak{A} \models \exists y\varphi[y/z]$.

O quantificador universal é tratado de forma completamente semelhante. □

O resultado desse teorema é que sempre se pode substituir uma variável ligada por uma "nova" variável, i.e. uma variável que não ocorria na fórmula. Disso se conclui facilmente que

**Corolário 2.5.7** *Toda fórmula é equivalente a uma outra fórmula na qual nenhuma variável ocorre ao mesmo tempo livre e ligada.*

Agora podemos puxar os quantificadores para a frente: $\forall x\varphi(x) \vee \forall x\psi(x) \leftrightarrow \forall x\varphi(x) \vee \forall y\psi(y)$ e $\forall x\varphi(x) \vee \forall y\psi(y) \leftrightarrow \forall xy(\varphi(x) \vee \psi(y))$, para um $y$ apropriado.

De modo a lidar com lógica de predicados de forma algébrica precisamos da técnica de substituição de equivalentes por equivalentes.

**Teorema 2.5.8 (Teorema da Substituição)**
(i) $\models t_1 = t_2 \rightarrow s[t_1/x] = s[t_2/x]$
(ii) $\models t_1 = t_2 \rightarrow \varphi[t_1/x] \leftrightarrow \varphi[t_2/x]$
(iii) $\models (\varphi \leftrightarrow \psi) \rightarrow (\sigma[\varphi/\$] \leftrightarrow \sigma[\psi/\$])$

*Demonstração.* Não é nenhuma restrição assumir que os termos e as fórmulas são fechados. Tacitamente assumimos que as substituições satisfazem as condições "livre para".

(i) Suponha que $\mathfrak{A} \models t_1 = t_2$, i.e. $t_1^{\mathfrak{A}} = t_2^{\mathfrak{A}}$. Agora use indução sobre $s$.

- $s$ é uma constante ou uma variável. Trivial.
- $s = \overline{F}(s_1, \ldots, s_k)$. Então $s[t_i/x] = \overline{F}(s_1[t_i/x], \ldots)$ e $(s[t_i/x])^{\mathfrak{A}} = F((s_1[t_i])^{\mathfrak{A}}/x, \ldots)$. Hipótese da indução: $(s_j[t_1/x])^{\mathfrak{A}} = (s_j[t_2/x])^{\mathfrak{A}}$, $1 \leq j \leq k$. Logo $(s[t_1/x])^{\mathfrak{A}} = F((s_1[t_1/x])^{\mathfrak{A}}, \ldots) = F((s_1[t_2/x])^{\mathfrak{A}}, \ldots) = (s[t_2/x]^{\mathfrak{A}})$. Portanto $\mathfrak{A} \models s[t_1/x] = s[t_2/x]$.

(ii) Suponha que $\mathfrak{A} \models t_1 = t_2$, logo $t_1^{\mathfrak{A}} = t_2^{\mathfrak{A}}$. Vamos mostrar que $\mathfrak{A} \models \varphi[t_1/x] \Leftrightarrow \mathfrak{A} \models \varphi[t_2/x]$ por indução sobre $\varphi$.

– $\varphi$ é atômica. O caso de um símbolo proposicional (incluindo $\perp$) é trivial. Portanto considere $\varphi = \overline{P}(s_1, \ldots, s_k)$. $\mathrm{A} \models \overline{P}(s_1, \ldots, s_k)[t_1/x] \Leftrightarrow \mathrm{A} \models \overline{P}(s_1[t_1/x], \ldots) \Leftrightarrow \langle (s_1[t_1/x])^{\mathrm{A}}, \ldots, (s_k[t_1/x])^{\mathrm{A}} \rangle \in P$. Pelo item (i), $(s_j[t_1/x])^{\mathrm{A}} = (s_j[t_2/x])^{\mathrm{A}}$, $j = 1, \ldots, k$.
  Logo obtemos $\langle (s_1[t_1/x])^{\mathrm{A}}, \ldots, \rangle \in P \Leftrightarrow \ldots \Leftrightarrow \mathrm{A} \models \overline{P}(s_1, \ldots)[t_2/x]$.

– $\varphi = \varphi_1 \vee \varphi_2$, $\varphi_1 \wedge \varphi_2$, $\varphi_1 \to \varphi_2$, $\neg\varphi_1$. Vamos considerar o caso da disjunção: $\mathrm{A} \models (\varphi_1 \vee \varphi_2)[t_1/x] \Leftrightarrow \mathrm{A} \models \varphi_1[t_1/x]$ ou $\mathrm{A} \models \varphi_2[t_1/x] \overset{h.i.}{\Leftrightarrow} \mathrm{A} \models \varphi_1[t_2/x]$ ou $\mathrm{A} \models \varphi_2[t_2/x] \Leftrightarrow \mathrm{A} \models (\varphi_1 \vee \varphi_2)[t_2/x]$.
  Os conectivos restantes são tratados semelhantemente.

– $\varphi = \exists y\psi$, $\varphi = \forall y\psi$.
  Vamos considerar o quantificador existencial. $\mathrm{A} \models (\exists y\psi)[t_1/x] \Leftrightarrow \mathrm{A} \models \exists y(\psi[t_1/x]) \Leftrightarrow \mathrm{A} \models \psi[t_1/x][\overline{a}/y]$ para algum $a$.
  Pelo Lema 2.5.4 $\mathrm{A} \models \psi[t_1/x][\overline{a}/y] \Leftrightarrow \mathrm{A} \models (\psi[\overline{a}/y])[t_1[\overline{a}/y]/x]$. Aplique a hipótese da indução a $\psi[\overline{a}/y]$ e aos termos $t_1[\overline{a}/y]$, $t_2[\overline{a}/y]$. Observe que $t_1$ e $t_2$ são termos fechados, portanto $t_1[\overline{a}/y] = t_1$ e $t_2[\overline{a}/y] = t_2$. Obtemos que $\mathrm{A} \models \psi[t_2/x][\overline{a}/y]$, e portanto $\mathrm{A} \models \exists y\psi[t_2/x]$. A outra direção é semelhante, assim como o caso do quantificador universal.

(iii) Suponha que $\mathrm{A} \models \varphi \Leftrightarrow \mathrm{A} \models \psi$. Vamos mostrar que $\mathrm{A} \models \sigma[\varphi/\$] \Leftrightarrow \mathrm{A} \models \sigma[\psi/\$]$ por indução sobre $\sigma$.

– $\sigma$ é atômica. Ambos os casos $\sigma = \$$ e $\sigma \neq \$$ são triviais.

– $\sigma = \sigma_1 \Box \sigma_2$ (ou $\neg\sigma_1$). Deixo ao leitor.

– $\sigma = \forall x\tau$. Observe que $\varphi$ e $\psi$ são fórmulas fechadas, mas mesmo se elas não o fossem $x$ poderia não ocorrer livre em $\varphi$, $\psi$.
  $\mathrm{A} \models (\forall x\tau)[\varphi/\$] \Leftrightarrow \mathrm{A} \models \forall x(\tau[\varphi/\$])$. Escolha um elemento $a \in |\mathrm{A}|$, então $\mathrm{A} \models (\tau[\varphi/\$])[\overline{a}/x] \overset{\clubsuit 2.5.4}{\Leftrightarrow} \mathrm{A} \models (\tau[\overline{a}/x])[\varphi[\overline{a}/x]/\$] \Leftrightarrow \mathrm{A} \models (\tau[\overline{a}/x])[\varphi/\$] \overset{h.i.}{\Leftrightarrow} \mathrm{A} \models \tau[\overline{a}/x][\psi/\$] \Leftrightarrow \mathrm{A} \models \tau[\overline{a}/x][\psi[\overline{a}/x]/\$] \Leftrightarrow \mathrm{A} \models (\tau[\psi/\$])[\overline{a}/x]$.
  Logo $\mathrm{A} \models \sigma[\varphi/\$] \Leftrightarrow \mathrm{A} \models \sigma[\psi/\$]$.
  O quantificador existencial é tratado de modo semelhante. $\Box$

Observe que na demonstração acima aplicamos indução sobre "$\sigma[\varphi/\$]$ para todo $\varphi$", porque a fórmula de substituição mudava durante o processo no caso do quantificador.

Note que $\sigma$ também mudava, por isso a rigor estamos aplicando indução sobre o posto (ou então temos que formular o princípio da indução 2.3.4 de modo um pouco mais liberal).

**Corolário 2.5.9**

(i) $[\![s[t/x]]\!] = [\![s[\overline{[\![t]\!]}/x]]\!]$
(ii) $[\![\varphi[t/x]]\!] = [\![\varphi[\overline{[\![t]\!]}/x]]\!]$

*Demonstração.* Vamos aplicar o Teorema da Substituição. Considere uma estrutura qualquer A. Note que $[\![\overline{[\![t]\!]}]\!] = [\![t]\!]$ (por definição), logo $\mathrm{A} \models \overline{[\![t]\!]} = t$. Agora (i) e (ii) seguem imediatamente. $\Box$

Usando uma notação mais frouxa, podemos escrever (i) e (ii) da seguinte forma:
$[\![s(t)]\!] = [\![s(\overline{[\![t]\!]})]\!]$, ou $\mathrm{A} \models s(t) = s(\overline{[\![t]\!]})$ e $[\![\varphi(t)]\!] = [\![\varphi(\overline{[\![t]\!]})]\!]$, ou $\mathrm{A} \models \varphi(t) \leftrightarrow \varphi(\overline{[\![t]\!]})$.

Observe que $[\![t]\!]$ $(= [\![t]\!]_{\mathrm{A}})$ é apenas uma outra maneira de escrever $t^{\mathrm{A}}$.

Demonstrações envolvendo análise detalhada da substituição são um bocado maçantes porém infelizmente inevitáveis. O leitor pode simplificar as demonstrações acima e outras do gênero supondo que as fórmulas envolvidas são todas fórmulas fechadas. Não há perda concreta de generalidade, pois apenas introduzimos um número de constantes de $L(\mathrm{A})$ e checamos se o resultado é válido para todas as escolhas de constantes.

Agora podemos realmente manipular fórmulas de uma forma algébrica. Novamente, escreva '$\varphi \mathrm{eq} \psi$' para designar $\models \varphi \leftrightarrow \psi$.

*Exemplos.*

1. $\forall x \varphi(x) \to \psi \mathrm{eq} \neg\forall x \varphi(x) \vee \psi \mathrm{eq} \exists x(\neg\varphi(x)) \vee \psi \mathrm{eq} \exists(\neg\varphi(x) \vee \psi) \mathrm{eq} \exists x(\varphi(x) \to \psi)$, onde $x \notin VL(\psi)$.

2. $\forall x \varphi(x) \to \exists x \varphi(x) \mathrm{eq} \neg\forall x \varphi(x) \vee \exists x \varphi(x) \mathrm{eq} \exists x(\neg\varphi(x) \vee \varphi(x))$. A fórmula no escopo do quantificador é verdadeira (já da lógica proposicional), logo a fórmula original é verdadeira.

**Definição 2.5.10** Uma fórmula $\varphi$ está na *forma (normal) prenex* se $\varphi$ consiste de uma cadeia (possivelmente vazia) de quantificadores seguida de uma fórmula aberta (i.e. livre-de-quantificador). Dizemos que $\varphi$ é uma fórmula prenex.

*Exemplos.* $\exists x \forall y \exists z \exists y(x = z \vee y = z \to v < y)$, $\forall x \forall y \exists z(P(x,y) \wedge Q(y,x) \to P(z,z))$.

Puxando os quantificadores para a frente da fórmula podemos reduzí-la a uma fórmula na forma prenex.

**Teorema 2.5.11** *Para cada $\varphi$ existe uma fórmula prenex $\psi$ tal que $\models \varphi \leftrightarrow \psi$.*

*Demonstração.* Primeiro elimine $\to$ e $\leftrightarrow$. Use indução sobre a fórmula resultante $\varphi'$.

Para $\varphi'$ atômica o teorema é trivial. Se $\varphi' = \varphi_1 \vee \varphi_2$ e $\varphi_1, \varphi_2$ são equivalentes a fórmulas prenex $\psi_1, \psi_2$ então

$\psi_1 = (Q_1 y_1) \ldots (Q_n y_n)\psi^1$,

$\psi_2 = (Q'_1 z_1) \ldots (Q'_m z_m)\psi^2$,

onde $Q_i, Q_j$ são quantificadores e $\psi^1, \psi^2$ são fórmulas abertas. Pelo Teorema 2.5.6 podemos escolher variáveis ligadas distintas, tomando cuidado para que nenhuma variável seja ao mesmo tempo livre e ligada. Aplicando o Teorema 2.5.3 encontramos

$\models \varphi' \leftrightarrow (Q_1 y_1) \ldots (Q_n y_n)(Q'_1 z_1) \ldots (Q'_m z_m)(\psi^1 \vee \psi^2)$,

e portanto chegamos aonde queríamos.

Os casos restantes deixo ao leitor. □

Em matemática é comum se pressupor que o leitor benévolo pode adivinhar as intenções do autor, não apenas as explícitas, mas também as que são tacitamente passadas através de gerações de matemáticos. Tome por exemplo a definição de convergência de uma seqüência: $\forall\varepsilon > 0\exists n\forall m(|a_n - a_{n+m}| > \varepsilon)$. De modo a fazer algum sentido dessa expressão é preciso acrescentar: as variáveis $n, m$ variam sobre o conjunto dos números naturais. Infelizmente nossa sintaxe não permite usar variáveis com sortes (tipos) diferentes. Daí como incorporarmos expressões do tipo acima? A resposta é simples: adicionamos predicados do sorte desejado e indicamos na fórmula a "natureza" da variável.

*Exemplo.* Seja $\mathrm{A} = \langle R, Q, < \rangle$ a estrutura dos reais com o conjunto dos números racionais destacado, provido com a ordem natural. A sentença $\sigma := \forall xy(x < y \to \exists z(Q(z) \wedge x < z \wedge z < y))$ pode ser interpretada em A da seguinte forma: $\mathrm{A} \models \sigma$, e ela nos diz que os racionais formam um conjunto denso nos reais (na ordenação natural). Achamos, entretanto, que esse modo de expressão é um pouco pesado. Por conseguinte introduzimos a noção de *quantificadores relativizados*. Como não importa se expressamos informalmente "$x$ é racional" através de $x \in Q$ ou de $Q(x)$, vamos facilitar nossas vidas e a cada vez escolher a notação que nos seja mais conveniente. Usaremos $(\exists x \in Q)$ e $(\forall x \in Q)$ como notação informal para "existe um $x$ em $Q$" e "para todo $x$ em $Q$". Agora vamos escrever $\sigma$ da forma $\forall xy(x < y \to \exists z \in Q(x < z \wedge z < y))$. Note que *não* escrevemos $(\forall xy \in R)(--)$, pois: (1) não existe relação $R$ em A, (e) as variáveis automaticamente variam sobre $|\mathrm{A}| = R$.

Vamos agora dar a definição propriamente dita da relativização de um quantificador:

**Definição 2.5.12** Se $P$ é um símbolo de predicado unário, então $(\forall x \in P)\varphi := \forall x(P(x) \to \varphi)$, $(\exists x \in P)\varphi := \exists x(P(x) \wedge \varphi)$.

Essa notação tem o significado pretendido, tal qual aparece de $\mathrm{A} \models (\forall x \in P)\varphi \Leftrightarrow$ para todo $a \in P^{\mathrm{A}}$ $\mathrm{A} \models \varphi[\overline{a}/x]$, $\mathrm{A} \models (\exists x \in P)\varphi \Leftrightarrow$ existe um $a \in P^{\mathrm{A}}$ tal que $\mathrm{A} \models \varphi[\overline{a}/x]$. A demonstração é imediata. Usaremos frequentemente notações informais, tais como $(\forall x > 0)$ ou $(\exists y \neq 1)$, que podem ser expressas da forma acima. O significado de tais notações estará sempre evidente. Pode-se restringir *todos* os quantificadores ao mesmo conjunto (predicado), e isso significa passar para um universo restrito (cf. Exercício 11).

É de conhecimento geral que ao fortalecer uma parte de uma conjunção (disjunção) a fórmula inteira é fortalecida, mas que ao fortalecer $\varphi$ em $\neg\varphi$ a fórmula inteira é enfraquecida. Esse fenômeno tem uma origem sintática, e introduziremos um pouco de terminologia para lidar com isso de maneira suave. Definimos indutivamente que uma ocorrência de uma subfórmula $\varphi$ é positiva (negativa) em $\sigma$:

**Definição 2.5.13** $Sub^+$ e $Sub^-$ são conjuntos definidos simultaneamente por:

$Sub^+(\varphi) = \{\varphi\}$
$Sub^-(\varphi) = \emptyset$ para $\varphi$ atômica
$Sub^+(\varphi_1 \Box \varphi_2) = Sub^+(\varphi_1) \cup Sub^+(\varphi_2) \cup \{\varphi_1 \Box \varphi_2\}$
$Sub^-(\varphi_1 \Box \varphi_2) = Sub^-(\varphi_1) \cup Sub^-(\varphi_2)$ para $\Box \in \{\wedge, \vee\}$
$Sub^+(\varphi_1 \to \varphi_2) = Sub^+(\varphi_1) \cup Sub^+(\varphi_2) \cup \{\varphi_1 \to \varphi_2\}$
$Sub^-(\varphi_1 \to \varphi_2) = Sub^+(\varphi_1) \cup Sub^-(\varphi_2)$

$Sub^+(Qx.\varphi) = Sub^+(\varphi) \cup \{Qx.\varphi\}$
$Sub^-(Qx.\varphi) = Sub^-(\varphi)$ para $Q \in \{\forall, \exists\}$

Se $\varphi \in Sub^+(\psi)$, então dizemos que $\varphi$ *ocorre positivamente* em $\psi$ (de modo semelhante para as ocorrências negativas).

Poderíamos ter-nos restringido a $\wedge, \rightarrow$ e $\forall$, mas não custa tanto espaço extra lidar com os outros conectivos.

O teorema seguinte esclarece as intuições básicas: se uma parte positiva de uma fórmula cresce em valor-verdade então a fórmula cresce em valor-verdade (ou melhor: não decresce em valor-verdade). Expressamos esse papel de subfórmulas positivas e negativas da seguinte maneira:

**Teorema 2.5.14** *Suponha que $\varphi$ ($\psi$) seja positiva (negativa) em $\sigma$, então:*
(i) $[\![\varphi_1]\!] \leq [\![\varphi_2]\!] \Rightarrow [\![\sigma[\varphi_1/\varphi]]\!] \leq [\![\sigma[\varphi_2/\varphi]]\!]$
(ii) $[\![\psi_1]\!] \leq [\![\psi_2]\!] \Rightarrow [\![\sigma[\psi_1/\varphi]]\!] \geq [\![\sigma[\psi_2/\varphi]]\!]$
(iii) $\mathrm{A} \models (\varphi_1 \rightarrow \varphi_2) \rightarrow (\sigma[\varphi_1/\varphi] \rightarrow \sigma[\varphi_2/\varphi])$
(iv) $\mathrm{A} \models (\psi_1 \rightarrow \varphi_2) \rightarrow (\sigma[\psi_2/\varphi] \rightarrow \sigma[\psi_1/\varphi])$.

*Demonstração.* Indução sobre $\sigma$. □

**Exercícios**

1. Mostre que todas as tautologias proposicionais são verdadeiras em todas as estruturas (do tipo de similaridade apropriado).

2. Suponha que $x \notin VL(\psi)$. Mostre que
   (i) $\models (\forall x\varphi \rightarrow \psi) \leftrightarrow \exists x(\varphi \rightarrow \psi)$,
   (ii) $\models (\exists x\varphi \rightarrow \psi) \leftrightarrow \forall x(\varphi \rightarrow \psi)$,
   (iii) $\models (\psi \rightarrow \exists x\varphi) \leftrightarrow \exists x(\psi \rightarrow \varphi)$,
   (iv) $\models (\psi \rightarrow \forall x\varphi) \leftrightarrow \forall x(\psi \rightarrow \varphi)$.

3. Mostre que a condição sobre $VL(\psi)$ no exercício 2 é necessária.

4. Mostre que $\not\models \forall x\exists y\varphi \leftrightarrow \exists y\forall x\varphi$.

5. Mostre que $\models \varphi \Rightarrow \models \forall x\varphi$ e $\models \exists x\varphi$.

6. Mostre que $\not\models \exists x\varphi \rightarrow \forall x\varphi$.

7. Mostre que $\not\models \exists x\varphi \wedge \exists x\psi \rightarrow \exists x(\varphi \wedge \psi)$.

8. Mostre que a condição sobre $x, y$ no Teorema 2.5.6 é necessária.

9. Mostre que
   (i) $\models \forall x(\varphi \rightarrow \psi) \rightarrow (\forall x\varphi \rightarrow \forall x\psi)$;
   (ii) $\models (\exists x\varphi \rightarrow \exists x\psi) \rightarrow \exists x(\varphi \rightarrow \psi)$;
   (iii) $\models \forall x(\varphi \leftrightarrow \psi) \rightarrow (\forall x\varphi \leftrightarrow \forall x\psi)$;
   (iv) $\models (\forall x\varphi \rightarrow \exists x\psi) \leftrightarrow \exists x(\varphi \rightarrow \psi)$;
   (v) $\models (\exists x\varphi \rightarrow \forall x\psi) \rightarrow \forall x(\varphi \rightarrow \psi)$.

10. Mostre que as recíprocas das implicações do exercício 9(i)–(iii) e (v) não se verificam.

11. Suponha que $L$ tenha um predicado unário $P$. Defina a relativização $\sigma^P$ de $\sigma$ por

$$\begin{array}{rcl} \sigma^P & := & \sigma \text{ para } \sigma \text{ atômica}, \\ (\varphi\Box\psi)^P & := & \varphi^P\Box\psi^P, \\ (\neg\varphi)^P & := & \neg\varphi^P, \\ (\forall x\varphi)^P & := & \forall x(P(x) \to \varphi^P), \\ (\exists x\varphi)^P & := & \exists x(P(x) \wedge \varphi^P). \end{array}$$

Seja A uma estrutura sem funç oes e sem constantes. Considere a estrutura B com universo $P^{\mathrm{A}}$ e relações que são restrições das relações de A, onde $P^{\mathrm{A}} \neq \emptyset$. Mostre que A $\models \sigma^P \Leftrightarrow$ B $\models \sigma$ para sentenças $\sigma$. Por que somente relações são permitidas em A?

12. Seja $S$ um símbolo de predicado binário. Mostre que $\models \neg\exists y\forall x(S(y,x) \leftrightarrow \neg S(x,x))$. (Pense na relação "$y$ barbeia $x$" e lembre-se do paradoxo do barbeiro de Russell).

13. (i) Mostre que as condições "livre para" não podem ser desprezadas em 2.5.8.

    (ii) Mostre que $\models t = s \Rightarrow \models \varphi[t/x] \leftrightarrow \varphi[s/x]$.

    (iii) Mostre que $\models \varphi \leftrightarrow \psi \Rightarrow \models \sigma[\varphi/\$] \leftrightarrow \sigma[\psi/\$]$.

14. Encontre a forma normal prenex de

    (a) $\neg((\neg\forall x\varphi(x) \vee \forall x\psi(x)) \wedge (\exists x\sigma(x) \to \forall x\tau(x)))$,

    (b) $\forall x\varphi(x) \leftrightarrow \exists x\psi(x)$,

    (c) $\neg(\exists x\varphi(x,y) \wedge (\forall y\psi(y) \to \varphi(x,x)) \to \exists x\forall y\sigma(x,y))$,

    (d) $((\forall x\varphi(x) \to \exists y\psi(x,y)) \to \psi(x,x)) \to \exists x\forall y\sigma(x,y)$.

15. Mostre que $\models \exists x(\varphi(x) \to \forall y\varphi(y))$. (É instrutivo pensar em $\varphi(x)$ como '$x$ bebe').

## 2.6 Identidade

Temos nos limitado nesse livro à consideração de estruturas com identidade, e portanto de linguagens com identidade. Por conseguinte classificamos '=' como um símbolo lógico, ao invés de um símbolo matemático. Podemos, entretanto, tratar = não apenas como um certo predicado binário, pois identidade satisfaz um número de axiomas característicos, listados abaixo.

$$\begin{array}{ll} I_1 & \forall x(x = x), \\ I_2 & \forall xy(x = y \to y = x), \\ I_3 & \forall xyz(x = y \wedge y = z \to x = z), \\ I_4 & \forall x_1 \ldots x_n y_1 \ldots y_n(\bigwedge_{i \leq n} x_i = y_i \to t(x_1, \ldots, x_n) = t(y_1, \ldots, y_n)), \\ & \forall x_1 \ldots x_n y_1 \ldots y_n(\bigwedge_{i \leq n} x_i = y_i \to \varphi(x_1, \ldots, x_n) = \varphi(y_1, \ldots, y_n)). \end{array}$$

Pode-se simplesmente checar que $I_1, I_2, I_3$ são verdadeiros, em toda estrutura A. No caso de $I_4$, observe que podemos supor que as fórmulas são fechadas.

Do contrário adicionamos quantificadores para cada variável restante e acrescentamos identidades postiças, e.g.

$$\forall z_1 \ldots z_k x_1 \ldots x_n y_1 \ldots y_n (\bigwedge_{i \le n} x_i = y_i \wedge \bigwedge_{i \le k} z_k = z_k \to t(x_1, \ldots, x_n) = t(y_1, \ldots, y_n)).$$

Agora $(t(\overline{a}_1, \ldots, \overline{a}_n))^{\mathrm{A}}$ define uma função $t^{\mathrm{A}}$ sobre $|\mathrm{A}|^n$, obtida a partir das funções dadas para A através de várias substituições, portanto $a_i = b_i (i \le n) \Rightarrow (t(\overline{a}_1, \ldots, \overline{a}_n))^{\mathrm{A}} = (t(\overline{b}_1, \ldots, \overline{b}_n))^{\mathrm{A}}$. Isso demonstra a primeira parte de $I_4$.

A segunda parte é demonstrada por indução sobre $\varphi$ (usando a primeira parte): e.g. considere o caso do quantificador universal e suponha que $a_i = b_i$ para todo $i \le n$.

$\mathrm{A} \models \forall u \varphi(u, \overline{a}_1, \ldots, \overline{a}_n) \Leftrightarrow \mathrm{A} \models \varphi(\overline{c}, \overline{a}_1, \ldots, \overline{a}_n)$ para todo $c \overset{h.i.}{\Leftrightarrow}$
$\mathrm{A} \models \varphi(\overline{c}, \overline{b}_1, \ldots, \overline{b}_n)$ para todo $c \Leftrightarrow \mathrm{A} \models \forall u \varphi(u, \overline{b}_1, \ldots, \overline{b}_n)$.

Logo $\mathrm{A} \models (\bigwedge_{i \le n} \overline{a}_i = \overline{b}_i) \Rightarrow \mathrm{A} \models \forall u \varphi(u, \overline{a}_1, \ldots, \overline{a}_n) \to \forall u \varphi(u, \overline{b}_1, \ldots, \overline{b}_n)$. Isso se verifica para todo $a_1, \ldots, a_n, b_1, \ldots, b_n$, logo $\mathrm{A} \models \forall x_1 \ldots x_n y_1 \ldots y_n (\bigwedge_{i \le n} x_i = y_i \to (\forall u \varphi(u, x_1, \ldots, x_n) \to \forall u \varphi(u, y_1, \ldots, y_n))$.

Note que $\varphi$ (respectivamente $t$), em $I_4$ pode ser qualquer fórmula (respectivamente termo), portanto $I_4$ permanece verdadeiro para um número infinito de axiomas. Denominamos tal "axioma instante" de *esquema de axioma*.

Os primeiros três axiomas enunciam que a identidade é uma relação de equivalência. $I_4$ enuncia que a identidade é uma congruência com respeito a todas as relações (definíveis).

É importante se dar conta de que somente a partir dos axiomas não podemos determinar a natureza precisa da relação de interpretação. Adotamos explicitamente a convenção de que "=" será sempre interpretada pela igualdade de fato.

## Exercícios

1. Mostre que $\models \forall x \exists y (x = y)$.
2. Mostre que $\models \forall x(\varphi(x) \leftrightarrow \exists y(x = y \wedge \varphi(y)))$ e que
   $\models \forall x(\varphi(x) \leftrightarrow \forall y(x = y \to \varphi(y)))$, onde $y$ não ocorre em $\varphi(x)$.
3. Mostre que $\models \varphi(t) \leftrightarrow \forall x(x = t \to \varphi(x))$ se $x \notin VL(t)$.
4. Mostre que as condições dos exercícios são necessárias.
5. Considere $\sigma_1 = \forall x(x \sim x)$, $\sigma_2 = \forall xy(x \sim y \to y \sim x)$, $\sigma_3 = \forall xyz(x \sim y \wedge y \sim z \to x \sim z)$. Mostre que se $\mathrm{A} \models \sigma_1 \wedge \sigma_2 \wedge \sigma_3$, onde $\mathrm{A} = \langle A, R \rangle$, então $R$ é uma relação de equivalência. Obs.: $x \sim y$ é uma notação sugestiva para o átomo $\overline{R}(x, y)$.
6. Seja $\sigma_4 = \forall xyz(x \sim y \wedge x \sim z \to y \sim z)$. Mostre que $\sigma_1, \sigma_4 \models \sigma_2 \wedge \sigma_3$.
7. Considere o esquema $\sigma_5 : x \sim y \to (\varphi[x/z] \to \varphi[y/z])$. Mostre que $\sigma_1, \sigma_5 \models \sigma_2 \wedge \sigma_3$. Obs.: se $\sigma$ é um esquema, então $\Delta \cup \{\sigma\} \models \varphi$ designa $\Delta \cup \Sigma \models \varphi$, onde $\Sigma$ consiste de todas as instâncias de $\sigma$.

8. Obtenha a versão-para-termos de $I_4$ a partir de sua versão-para-fórmulas.

## 2.7 Exemplos

Consideraremos linguagens para alguns tipos familiares de estruturas. Como todas as linguagens são construídas da mesma maneira, não listaremos os símbolos lógicos. Supõe-se que todas as estruturas satisfazem os axiomas da identidade $I_1$–$I_4$. Para um refinamento veja 2.10.2.

**1. *A linguagem da identidade.*** Tipo: $\langle -; -; 0\rangle$.

*Alfabeto.*

Símbolo de predicado: $=$

As estruturas desse tipo são da forma $\mathfrak{A} = \langle A\rangle$, e satisfazem $I_1, I_2, I_3$. (Nessa linguagem $I_4$ segue de $I_1, I_2, I_3$, cf. 2.10 Exercício 5).

Em uma estrutura somente com a identidade existe tão pouca "estrutura" que tudo o que se pode fazer é olhar para o número de elementos (cardinalidade). Existem sentenças $\lambda_n$ e $\mu_n$ dizendo que existem pelo menos (ou, no máximo) $n$ elementos (Exercício 3, seção 3.1)

$$\lambda_n := \exists y_1 \dots y_n \bigwedge_{i\neq j} y_i \neq y_j, (n > 1),$$
$$\mu_n := \forall y_1 \dots y_n \bigvee_{i\neq j} y_i \neq y_j, (n > 0).$$

Portanto $\mathfrak{A} \models \lambda_n \wedge \mu_n$ sse $|\mathfrak{A}|$ tem exatamente $n$ elementos. Como universos não são vazios $\models \exists x(x = x)$ sempre se verifica.

Podemos também formular "*existe um único $x$ tal que ...*".

**Definição 2.7.1** $\exists! x\varphi(x) := \exists x(\varphi(x) \wedge \forall y(\varphi(y) \to x = y))$, onde $y$ não ocorre em $\varphi(x)$.

Note que $\exists! x\varphi(x)$ é uma abreviação (informal).

**2. *A linguagem da ordem parcial.*** Tipo: $\langle 2; -; 0\rangle$.

*Alfabeto.*

Símbolos de predicado: $=, \leq$.

| | | |
|---|---|---|
| *Abreviações* | $x \neq y := \neg x = y$, | $x < y := x \leq y \wedge x \neq y$, |
| | $x > y := y < x$, | $x \geq y := y \leq x$, |
| | $x \leq y \leq z := x \leq y \wedge y \leq z$. | |

**Definição 2.7.2** $\mathfrak{A}$ é um *conjunto parcialmente ordenado (poset)* se $\mathfrak{A}$ é um modelo de

$\forall xyz(x \leq y \leq z \to x \leq z)$,

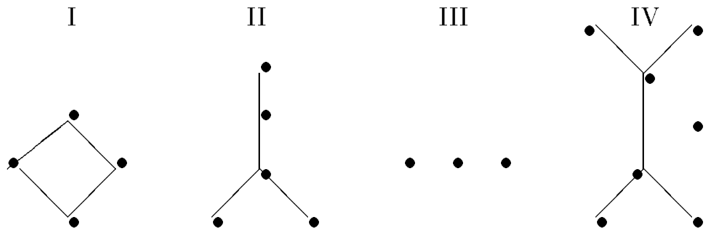
$\forall xy(x \leq y \leq x \leftrightarrow x = y)$.

A notação pode confundir, pois usualmente se introduz a relação $\leq$ (e.g. sobre os reais) como uma disjunção $x < y$ ou $x = y$. Em nosso alfabeto a relação é primitiva, embora um outro símbolo teria sido preferível, mas decidimos seguir a tradição. Note que a relação é reflexiva: $x \leq x$.

Conjuntos parcialmente ordenados são bem básicos em matemática, pois aparecem sob várias formas. É muitas vezes conveniente visualizar *posets* por meio de diagramas, onde $a \leq b$ é representado como igual ou acima (respectivamente à direita). Uma das tradições em lógica é a de manter objetos e seus nomes separadamente. Por conseguinte falamos de símbolos de função que são interpretados por funções, etc. Entretanto, na prática isso torna a notação um pouco carregada. Preferimos usar a mesma notação para os objetos sintáticos e suas interpretações, e.g. se $\mathrm{R} = \langle \mathbb{R}, \leq \rangle$ é o conjunto parcialmente ordenado dos números reais, então $\mathrm{R} \models \forall x \exists y (x \leq y)$, enquanto que a rigor deveria ser escrito algo como $\forall x \exists y (x \overline{\leq} y)$ para distinguir o símbolo da relação que o interpreta.

O símbolo '$\leq$' em R representa a relação propriamente dita e o '$\leq$' na sentença é o símbolo de predicado. Recomenda-se que o leitor distinga os símbolos em suas várias apresentações.

Mostramos alguns diagramas de *posets*.




Dos diagramas podemos extrair um bocado de propriedades. E.g. $\mathrm{A}_1 \models \exists x \forall y (x \leq y)$ ($\mathrm{A}_i$ é a estrutura com o diagrama da figura $i$), i.e. $\mathrm{A}_1$ tem um elemento mínimo. $\mathrm{A}_3 \models \forall x \neg \exists y (x < y)$, i.e. em $\mathrm{A}_3$ nenhum elemento é estritamente menor que um outro elemento.

**Definição 2.7.3** (i) A é um *conjunto (linearmente ou totalmente) ordenado* se ele é um poset e $\mathrm{A} \models \forall xy (x \leq y \vee y \leq x)$ (cada dois elementos são comparáveis).

(ii) A é *densamente ordenado* se $\mathrm{A} \models \forall xy (x < y \rightarrow \exists z (x < z \wedge z < y))$ (entre dois elementos quaisquer existe um terceiro elemento).

Um exercício razoavelmente divertido é encontrar sentenças que distinguem entre estruturas e vice-versa. Por exemplo podemos distinguir $\mathrm{A}_3$ e $\mathrm{A}_4$ (do diagrama acima) da seguinte maneira: em $\mathrm{A}_4$ existe precisamente *um* elemento que é incomparável a todos os outros elementos, em $\mathrm{A}_3$ existem mais de um elementos como esse. Ponha $\sigma(x) := \forall y (y \neq x \rightarrow \neg y \leq x \wedge \neg x \leq y)$. Então $\mathrm{A}_4 \models \forall xy (\sigma(x) \wedge \sigma(y) \rightarrow x = y)$, porém $\mathrm{A}_3 \models \neg \forall xy (\sigma(x) \wedge \sigma(y) \rightarrow x = y)$.

**3.** ***A linguagem dos grupos.*** Tipo: $\langle -; 2, 1; 1 \rangle$.

*Alfabeto.*

Símbolo de predicado: $=$
Símbolos de função: $\cdot$, $^{-1}$
Símbolos de constante: $e$

Notação: De modo a estar de acordo a prática escrevemos $t \cdot s$ e $t^{-1}$ ao invés de $\cdot(t, s)$ e $^{-1}(t)$.

**Definição 2.7.4** A é *grupo* se ele é um modelo de
$\forall xyz((x \cdot y) \cdot z) = x \cdot (y \cdot z))$,
$\forall x(x \cdot e = x \wedge e \cdot x = x)$,
$\forall x(x \cdot x^{-1} = e \wedge x^{-1} \cdot x = e)$.

Quando conveniente, escreveremos $ts$ para designar $t \cdot s$; adotaremos as convenções de parentização da álgebra. Um grupo A é *comutativo* ou *abeliano* se $A \models \forall xy(xy = yx)$.

Grupos comutativos são frequentemente descritos na linguagem dos grupos *aditivos*, que têm o seguinte alfabeto:

Símbolo de predicado: $=$
Símbolos de função: $+$, $-$
Símbolos de constante: $0$

**4. *A linguagem da geometria projetiva plana.*** Tipo: $\langle 2; -; 0\rangle$.

As estruturas que se considera neste caso são planos projetivos, que são usualmente assumidos como consistindo de *pontos* e *retas* com uma *relação de incidência*. Nessa abordagem o tipo seria $\langle 1, 1, 2; -; 0\rangle$. Podemos, entretanto, usar um tipo mais simples, já que um ponto pode ser definido como algo que é incidente a uma reta, e uma reta como algo para o qual podemos encontrar um ponto que lhe é incidente. Obviamente isso requer uma relação de incidência não-simétrica.

Agora relacionaremos os axiomas, que divergem um pouco do conjunto tradicional de axiomas. É um exercício simples mostrar que o sistema é equivalente aos conjuntos tradicionais.

*Alfabeto.*

Símbolos de predicado: $I$, $=$.

Introduzimos as seguintes abreviações:
$\Pi(x) := \exists y(xIy)$, $\qquad \Lambda(y) := \exists x(xIy)$.

**Definição 2.7.5** A é *plano projetivo* se satisfaz
$\gamma_0$ : $\forall x(\Pi(x) \leftrightarrow \neg\Lambda(x))$,
$\gamma_1$ : $\forall xy(\Pi(x) \wedge \Pi(y) \to \exists z(xIz \wedge yIz)$,
$\gamma_2$ : $\forall uv(\Lambda(u) \wedge \Lambda(v) \to \exists x(xIu \wedge xIv))$,
$\gamma_3$ : $\forall xyuv(xIu \wedge yIu \wedge xIv \wedge yIv \to x = y \vee u = v)$,
$\gamma_4$ : $\exists x_0x_1x_2x_3u_0u_1u_2u_3(\bigwedge x_iIu_i \wedge \bigwedge_{j=i-1(\text{mod}3)} x_iIu_j \wedge \bigwedge_{j\neq i-1(\text{mod}3)} \neg x_iIu_j)$.

$\gamma_0$ nos diz que em um plano projetivo tudo é ponto, ou reta; $\gamma_1$ e $\gamma_2$ nos dizem que "quaisquer duas retas se intersectam em um ponto" e "quaisquer dois pontos podem ser unidos por uma reta", por $\gamma_3$ esse ponto (ou reta) é único se as dadas retas (ou os dados pontos) são distintas (ou distintos). Finalmente $\gamma_4$

torna os planos projetivos não-triviais, no sentido de que existem pontos e retas em número suficiente.

$\Pi^{\mathrm{A}} = \{a \in |\mathrm{A}| \mid \mathrm{A} \models \Pi(\overline{a})\}$ e $\Lambda^{\mathrm{A}} = \{b \in |\mathrm{A}| \mid \mathrm{A} \models \Lambda(\overline{b})\}$ são os conjuntos de *pontos* e *retas* de A; $I^{\mathrm{A}}$ é a *relação de incidência* em A.

A formalização acima é um bocado complicada. Normalmente se usa um formalismo bi-sortido, com $P, Q, R, \ldots$ variando sobre pontos e $\ell, m, n \ldots$ variando sobre retas. O primeiro axioma é então omitido por convenção. Os axiomas restantes ficam assim

$$\begin{array}{ll}
\gamma_1' & : \forall PQ\exists\ell(PI\ell \wedge QI\ell),\\
\gamma_2' & : \forall\ell m\exists P(PI\ell \wedge PIm),\\
\gamma_3' & : \forall PQ\ell m(PI\ell \wedge QI\ell \wedge PIm \wedge QIm \to P = Q \vee \ell = m),\\
\gamma_4' & : \exists P_0P_1P_2P_3\ell_0\ell_1\ell_2\ell_3(\bigwedge P_iI\ell_i \wedge \displaystyle\bigwedge_{j=i-1(\mathrm{mod}3)} P_iI\ell_i \wedge \bigwedge_{\substack{j\neq i-1(\mathrm{mod}3)\\ i\neq j}} \neg P_iI\ell_j).
\end{array}$$

A tradução de uma linguagem para a outra não apresenta qualquer dificuldade. Os axiomas acima são diferentes dos axiomas usualmente dados no curso de geometria projetiva. Escolhemos esses axiomas específicos porque são fáceis de formular e também porque o chamado *princípio da dualidade* segue imediatamente. (cf. 2.10, Exercício 8). O quarto axioma é um axioma de extensão, e simplesmente diz que certas coisas existem; ele pode ser parafraseado diferentemente: existem quatro pontos entre os quais não há um grupo de três pontos colineares (i.e. sobre uma reta). Tal axioma de extensão é meramente uma precaução para assegurar que modelos triviais sejam excluídos. Nesse caso particular, não se poderia fazer muita geometria se houvesse apenas um triângulo!

**5.** ***A linguagem dos anéis com elemento unitário.*** Tipo: $\langle -; 2, 2, 1; 2\rangle$.

*Alfabeto.*

Símbolo de predicado: $=$
Símbolos de função: $+, \cdot, -$
Símbolos de constante: $0, 1$

**Definição 2.7.6** A é um *anel* (com elemento unitário) se ele é um modelo de
$\forall xyz((x + y) + z = x + (y + z))$,
$\forall xy(x + y = y + x)$,
$\forall xyz((x \cdot y) \cdot z = x \cdot (y \cdot z))$,
$\forall xyz(x \cdot (y + z) = x \cdot y + x \cdot z)$,
$\forall x(x + 0 = x)$,
$\forall x(x + (-x) = 0)$,
$\forall x(1 \cdot x = x \wedge x \cdot 1 = x)$,
$0 = 1$.

Um anel A é *comutativo* se $\mathrm{A} \models \forall xy(x \cdot y = y \cdot x)$.
Um anel A é um *anel de divisão* se $\mathrm{A} \models \forall x(x \neq 0 \to \exists y(x \cdot y = 1))$.
Um anel comutativo de divisão é chamado de *corpo*.

Na verdade é mais conveniente se ter disponível na linguagem de corpos, um símbolo para a função que dá o elemento inverso, daí a linguagem teria o tipo

$\langle -; 2, 2, 1, 1; 2\rangle$.
Por conseguinte adicionamos à lista anterior de axiomas as sentenças
$\forall x(x \neq 0 \rightarrow x \cdot x^{-1} = 1 \wedge x^{-1} \cdot x = 1)$ e $0^{-1} = 1$.

Note que devemos de alguma maneira "fixar o valor de $0^{-1}$", e a razão para isso aparecerá em 2.10, Exercício 2.

**6.** ***A linguagem da aritmética.*** Tipo: $\langle -; 2, 2, 1; 1\rangle$.

*Alfabeto.*

Símbolo de predicado: $=$
Símbolos de função: $+$, $\cdot$, $S$
Símbolo de constante: $0$
($S$ representa a função sucessor $n \mapsto n + 1$).

Historicamente, a linguagem da aritmética foi introduzida por Peano com a intenção de descrever os números naturais com adição, multiplicação e sucessor, a menos de isomorfismo. Isso em contraste com, e.g. a teoria dos grupos, na qual se procura capturar uma grande classe de estruturas não-isomorfas. Aconteceu, entretanto, que os axiomas de Peano caracterizaram uma grande classe de estruturas, que chamaremos (na falta de um termo) *estruturas de Peano*. Sempre que alguma confusão ameaça acontecer usaremos a notação oficial para o símbolo zeo: $\overline{0}$, porém na maioria das vezes confiaremos no bom senso do leitor.

**Definição 2.7.7** Uma *estrutura de Peano* $\mathfrak{A}$ é um modelo de
$\forall x(0 \neq S(x))$,
$\forall xy(S(x) = S(y) \rightarrow x = y)$,
$\forall x(x + 0 = x)$,
$\forall xy(x + S(y) = S(x + y))$,
$\forall x(x \cdot 0 = 0)$,
$\forall xy(x \cdot S(y) = x \cdot y + x)$,
$\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(S(x))) \rightarrow \forall x\varphi(x)$.

O último esquema de axioma é chamado *esquema de indução* ou *princípio da indução matemática*.

Será útil dispor de um pouco mais de notação. Definimos:
$\overline{1} := S(\overline{0})$, $\overline{2} := S(\overline{1})$, e em geral $\overline{n+1} := S(\overline{n})$,
$x < y := \exists z(x + Sz = y)$,
$x \leq y := x < y \vee x = y$.

Existe uma estrutura de Peano que é o modelo pretendido da aritmética, a saber a estrutura usual dos números naturais, com as operações usuais de adiçã, multiplicação e sucessor (e.g. os ordinais finitos na teoria dos conjuntos). Chamamos essa estrutura de Peano de *modelo padrão* $\mathfrak{N}$, e os números naturais usuais são chamados de *números padrão*.

Verifica-se facilmente que $\overline{n}^{\mathfrak{N}} = n$ e que $\mathfrak{N} \models \overline{n} < \overline{m} \Leftrightarrow n < m$: pela definição de interpretação temos que $\overline{0}^{\mathfrak{N}} = 0$. Assuma que $\overline{n}^{\mathfrak{N}} = n$, $\overline{n+1}^{\mathfrak{N}} = (S(\overline{n}))^{\mathfrak{N}} = \overline{n}^{\mathfrak{N}} + 1 = n + 1$. Agora aplicamos a indução matemática na meta-linguagem, e obtemos que $\overline{n}^{\mathfrak{N}} = n$ para todo $n$. Para a segunda alegação veja o Exercício 13. Em $\mathfrak{N}$ podemos definir todos os tipos de conjuntos, relações e números. Para ser mais preciso dizemos que uma relação $k$-ária $R$ em $\mathfrak{N}$ é definida por $\varphi$ se

$\langle a_1, \ldots, a_k \rangle \in R \Leftrightarrow \mathrm{N} \models \varphi(\overline{a_1}, \ldots, \overline{a_k})$. Um elemento $a \in |\mathrm{N}|$ é definido em N por $\varphi$ se $\mathrm{N} \models \varphi(\overline{b}) \Leftrightarrow b = a$, ou $\mathrm{N} \models \forall x(\varphi(x) \leftrightarrow x = \overline{a})$.

*Exemplos.*
(a) O conjunto dos números pares é definido por $P(x) := \exists y(x = y + y)$.
(b) A relação de divisibilidade é definida por $x|y := \exists z(xz = y)$.
(c) O conjunto dos números primos é definido por $Pr(x) := \forall yz(x = yz \rightarrow y = 1 \vee z = 1) \wedge x \neq 1$.

Podemos dizer que introduzimos os predicados $P$, $|$ e $Pr$ por definição (explícita).

**7. *A linguagem dos grafos.***
Usualmente pensamos em grafos como figuras geométricas consistindo de vértices e arestas conectando alguns dos vértices. Uma linguagem adequada para a teoria dos grafos é obtida introduzindo-se um predicado $R$ que expressa o fato de que dois vértices estão conectados por uma aresta. Daí, não precisamos de variáveis ou constantes para arestas.

*Alfabeto.*

Símbolos de predicado: $R$, $=$.

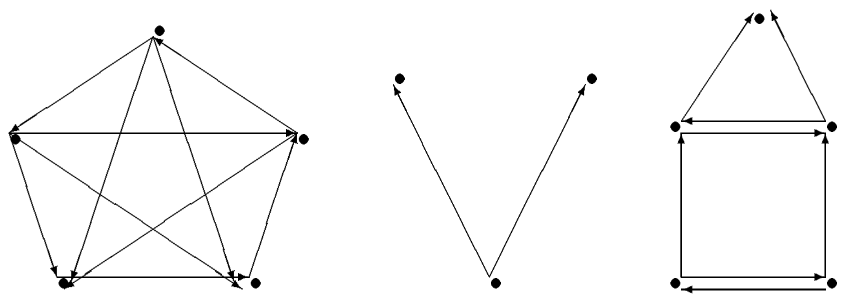
**Definição 2.7.8** Um *grafo* é uma estrutura $\mathrm{A} = \langle A, R \rangle$ satisfazendo os seguintes axiomas:
$\forall xy(R(x,y) \rightarrow R(y,x))$,
$\forall x \neg R(x,x)$.

Essa definição está de acordo com a tradição geométrica. Existem elementos, chamados vértices, dos quais alguns são conectados por arestas. Note que dois vértices são conectados por no máximo uma aresta. Além do mais, não há (necessidade de haver uma) aresta de um vértice para si próprio. Isso é inspirado na geometria, entretanto, do ponto de vista das numerosas aplicações de grafos parece que noções mais liberais são desejadas.

*Exemplos.*

Podemos também considerar grafos nos quais as arestas são direcionadas. Um *grafo direcionado* $\mathrm{A} = \langle A, R \rangle$ satisfaz apenas ao axioma $\forall x \neg R(x,x)$.

*Exemplos.*



Se abandonamos a condição de irreflexividade então um "grafo" é simplesmente um conjunto com uma relação binária. Podemos generalizar a noção ainda mais, de forma que mais arestas podem conectar um par de vértices.

Para tratar tais grafos generalizados consideramos uma linguagem com dois predicados unários $V, E$ e um predicado ternário $C$. Pense em $V(x)$ como "$x$ é um vértice". $E(x)$ como "$x$ é uma aresta", e $C(x, z, y)$ como "$z$ conecta $x$ e $y$". Um *multigrafo* direcionado é uma estrutura $= \langle A, V, E, C\rangle$ satisfazendo os seguintes axiomas:

$\forall x(V(x) \leftrightarrow \neg E(x))$,

$\forall xyz(C(x, z, y) \rightarrow V(x) \wedge V(y) \wedge E(z))$.

As arestas podem ser vistas como setas. Adicionando a condição de simetria, $\forall xyz(C(x, z, y) \rightarrow C(y, z, x))$ obtém-se multigrafos não-direcionados.

*Exemplos.*

figuras da página 90

**Observação:** A nomenclatura em teoria dos grafos não é muito uniforme. Escolhemos nosso arcabouço formal de tal forma que ele se preste ao tratamento em lógica de primeira ordem.

Para o propósito de descrever multigrafos uma linguagem bi-sortida (cf. geometria) é bem adequada. Deixo a reformulação ao leitor.

**Exercícios**

1. Considere a linguagem das ordens parciais. Defina predicados para $(a)$ $x$ é o *máximo*; $(b)$ $x$ é *maximal*; $(c)$ não existe elemento entre $x$ e $y$; $(d)$ $x$ é um *sucessor imediato* (respectivamente *predecessor imediato*) de $y$; $(e)$ $z$ é o *ínfimo* de $x$ e $y$.

2. Dê uma sentença $\sigma$ tal que $\mathrm{A}_2 \models \sigma$ e $\mathrm{A}_4 \models \neg\sigma$ (para $\mathrm{A}_i$ associado aos diagramas da página ??).

3. Sejam $\mathrm{A}_1 = \langle \mathbb{N}, \leq\rangle$ e $\mathrm{A}_2 = \langle \mathbb{Z}, \leq\rangle$ os conjuntos ordenados dos números naturais, e dos inteiros, respectivamente. Dê uma sentença $\sigma$ tal que $\mathrm{A}_1 \models \sigma$ e $\mathrm{A}_2 \models \neg\sigma$. Faça o mesmo para $\mathrm{A}_2$ e $\mathrm{B} = \langle \mathbb{Q}, \leq\rangle$ (o conjunto ordenado dos racionais). Obs.: $\sigma$ está na linguagem dos posets; em particular, você não pode adicionar constantes ou símbolos de função, etc., embora que abreviações definidas sejam obviamente bastante úteis.

4. Seja $\sigma = \exists x \forall y(x \leq y \vee y \leq x)$. Encontre posets A e B tais que $\mathrm{A} \models \sigma$ e $\mathrm{B} \models \neg\sigma$.

5. Faça o mesmo para $\sigma = \forall xy \exists z((x \leq z \wedge y \leq z) \vee (z \leq x \wedge z \leq y))$.

6. Usando a linguagem da identidade dê um conjunto (infinito) $\Gamma$ tal que A seja um modelo de $\Gamma$ sse A for infinito.

7. Considere a linguagem dos grupos. Defina as propriedades: (a) $x$ é idempotente; (b) $x$ pertence ao centro.

8. Seja A um anel; dê uma sentença $\sigma$ tal que $\mathrm{A} \models \sigma \Leftrightarrow \mathrm{A}$ é um domínio integral (i.e. não tem divisores de zero).

9. Dê uma fórmula $\sigma(x)$ na linguagem dos anéis tal que $\mathrm{A} \models \sigma(\overline{a}) \Leftrightarrow$ o ideal principal $(a)$ é primo (em A).

10. Defina na linguagem da aritmética: (a) $x$ e $y$ são primos entre si; (b) $x$ é o menor primo maior que $y$; (c) $x$ é o maior número com $2x < y$.

11. $\sigma := \forall x_1 \ldots x_n \exists y_1 \ldots y_m \varphi$ e $\tau := \exists y_1 \ldots y_m \psi$ são sentenças em uma linguagem sem a identidade, símbolos de função ou constantes, onde $\varphi$ e $\psi$ são livres de quantificador. Mostre que: $\models \sigma \Leftrightarrow \sigma$ se verifica em todas as estruturas com $n$ elementos. $\models \tau \Leftrightarrow \tau$ se verifica em todas as estruturas com 1 elemento.

12. O *cálculo monádico de predicados* tem apenas símbolos unários de predicado (sem a identidade). Considere $\mathrm{A} = \langle A, R_1, \ldots, R_n \rangle$ onde todos os $R_i$'s são conjuntos. Defina $a \sim b := a \in R_i \Leftrightarrow b \in R_i$ para todo $i \leq n$. Mostre que $\sim$ é uma relação de equivalência e que $\sim$ tem no máximo $2^n$ classes de equivalência. A classe de equivalência de $a$ é representada por $[a]$. Defina $B = A/\sim$ e $[a] \in S_i \Leftrightarrow a \in R_i$, $\mathrm{B} = \langle B, S_1, \ldots, S_n \rangle$. Mostre que $\mathrm{A} \models \sigma \Leftrightarrow \mathrm{B} \models \sigma$ para toda $\sigma$ na linguagem correspondente. Para tal $\sigma$ mostre que $\models \sigma \Leftrightarrow \mathrm{A} \models \sigma$ para toda A com no máximo $2^n$ elementos. Usando esse fato, esquematize um procedimento de decisão para a noção de verdade no cálculo monádico de predicados.

13. Seja N o modelo padrão da aritmética. Mostre que $\mathrm{N} \models \overline{n} < \overline{m} \Leftrightarrow n < m$.

14. Seja $\mathrm{N} = \langle \mathbb{N}, < \rangle$ e $\mathrm{B} = \langle \mathbb{N}, \triangle \rangle$, onde $n \triangle m$ sse (i) $n < m$ e $n$, $m$ são ambos pares ou ambos ímpares, ou (ii) se $n$ é par e $m$ é ímpar. Dê uma sentença $\sigma$ tal que $\mathrm{A} \models \sigma$ e $\mathrm{B} \models \neg\sigma$.

15. Se $\langle A, R \rangle$ é um plano projetivo, então $\langle A, \breve{R} \rangle$ também é um plano projetivo (*o plano dual*), onde $\breve{R}$ é a relação inversa da relação $R$. Formulando na linguagem bi-sortida: se $\langle A_P, A_L, I \rangle$ é um plano projetivo, então $\langle A_L, A_P, \breve{I} \rangle$ também o é.)

## 2.8 Dedução Natural

Estendemos o sistema da seção 1.5 para a lógica de predicados. Por razões semelhantes às mencionadas na seção 1.5 consideramos a linguagem com os conectivos $\wedge$, $\rightarrow$, $\perp$ e $\forall$. O quantificador existencial é deixado de fora, porém ele será considerado mais adiante.

Adotamos todas as regras da lógica proposicional e adicionamos

$$\forall I \frac{\varphi(x)}{\forall x \varphi(x)} \qquad \forall E \frac{\forall x \varphi(x)}{\varphi(t)}$$

tal que na regra $\forall I$ a variável $x$ não pode ocorrer em qualquer hipótese da qual $\varphi(x)$ depende, i.e. uma hipótese não-cancelada na derivação de $\varphi(x)$. Em $\forall E$ exigimos, é claro, que $t$ seja livre para $x$.

$\forall I$ tem a seguinte explicação intuitiva: se um objeto arbitrário $x$ tem a propriedade $\varphi$, então todo objeto tem a propriedade $\varphi$. O problema é que nenhum dos objetos que conhecemos em matemática pode ser considerado "arbitrário". Portanto ao invés de procurar pelo "objeto arbitrário" no mundo real (do ponto de vista da matemática), vamos tentar encontrar um critério sintático. Considere uma variável $x$ (ou uma constante) em uma derivação, existem fundamentos razoáveis para chamar $x$ de "arbitrário"? Aqui vai uma sugestão plausível: no contexto das derivações chamaremos $x$ *arbitrário* se nada foi assumido concernente a $x$. Em termos mais técnicos, $x$ é arbitrário em sua ocorrência específica em uma derivação se a parte da derivação acima dela não contém qualquer hipótese que contenha $x$ livre.

Demonstraremos a necessidade das restrições acima, lembrando sempre que o sistema pelo menos tem que ser *seguro*, i.e. que enunciados deriváveis devem ser verdadeiros.

Restrição sobre $\forall I$:

$$\dfrac{\dfrac{\dfrac{\dfrac{[x=0]}{\forall x(x=0)}}{x=0\rightarrow\forall x(x=0)}}{\forall x(x=0\rightarrow\forall x(x=0))}}{0=0\rightarrow\forall x(x=0)}$$

A introdução do $\forall$ no primeiro passo foi ilegal.

Logo $\vdash 0=0\rightarrow\forall x(x=0)$, porém claramente $\not\models 0=0\rightarrow\forall x(x=0)$ (tome qualquer estrutura contendo mais que apenas o 0).

Restrição sobre $\forall E$:

$$\begin{array}{c} [\forall x\neg\forall y(x=y)] \\ \hline \\ \hline \neg\forall y(y=y) \\ \hline \forall x\neg\forall y(x=y)\rightarrow\neg\forall y(y=y) \end{array}$$

A eliminação do $\forall$ no primeiro passo foi ilegal.

Note que $y$ não é livre para $x$ em $\neg\forall y(x=y)$. A sentença derivada é claramente falsa em estruturas com pelo menos dois elementos.

Agora vamos dar alguns exemplos de derivações. Assumimos que o leitor nesse ponto tenha experiência suficiente em cancelar hipóteses, de tal forma que não mais indicaremos os cancelamentos usando números.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\forall x\forall y\varphi(x,y)]}{\forall y\varphi(x,y)}\,\forall E}{\varphi(x,y)}\,\forall E}{\forall x\varphi(x,y)}\,\forall I}{\forall y\forall x\varphi(x,y)}\,\forall I}{\forall x\forall y\varphi(x,y)\rightarrow\forall y\forall x\varphi(x,y)}\rightarrow I \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\forall x(\varphi(x)\wedge\psi(x))]}{\varphi(x)\wedge\psi(x)}}{\varphi(x)}}{\forall x\varphi(x)} \quad \dfrac{\dfrac{\dfrac{[\forall x(\varphi(x)\wedge\psi(x))]}{\varphi(x)\wedge\psi(x)}}{\psi(x)}}{\forall x\psi(x)}}{\forall x\varphi(x)\wedge\forall x\psi(x)}}{\forall x(\varphi\wedge\psi)\rightarrow\forall x\varphi\wedge\forall x\psi}$$

Seja $x \notin VL(\varphi)$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\forall x(\varphi \to \psi(x))]}{\varphi \to \psi(x)}\forall E \qquad [\varphi]}{\psi(x)} \to E}{\forall x \psi(x)} \forall I}{}}{\varphi \to \forall x \psi(x)} \to I}{\forall x(\varphi \to \psi(x)) \to (\varphi \to \forall x \psi(x))} \to I
\qquad
\dfrac{\dfrac{[\varphi]}{\forall x \varphi}\forall I \qquad \dfrac{[\forall x \varphi]}{\varphi}\forall E}{\varphi \leftrightarrow \forall x \varphi}
$$

Na derivação mais à direita $\forall I$ foi permitido, pois $x \notin VL(\varphi)$, e $\forall E$ é aplicável.

Note que $\forall I$ na derivação mais à esquerda é permitido porque $x \notin VL(\varphi)$, pois naquele ponto $\varphi$ é ainda (parte de) uma hipótese.

O leitor terá absorvido a técnica por trás das regras dos quantificadores: reduza um $\forall x \varphi$ e reintroduza $\forall$ mais adiante, se necessário. Intuitivamente, procede-se da seguinte maneira: para mostrar que "para todo $x \ldots x \ldots$" basta mostrar que "$\ldots x \ldots$" para um $x$ arbitrário. Esse último enunciado é mais fácil de manusear. Sem entrar em distinções filosóficas mais apuradas, notamos que a distinção "para todo $x \ldots x \ldots$" – "para um $x$ arbitrário $\ldots x \ldots$" está embutido no nosso sistema por meio da distinção "enunciado quantificado" – "enunciado com variável livre".

O leitor terá também observado que sob uma estratégia razoável de derivação, a grosso modo, eliminação precede introdução. Existe uma explicação segura para esse fenômeno, seu tratamento apropriado pertencendo à *teoria da prova*, onde *derivações normais* (derivações sem passos supérfluos) são consideradas. Veja o Capítulo 6. No momento o leitor pode aceitar o fato mencionado acima como uma regra-do-polegar conveniente.

Podemos formular as propriedades de derivabilidade do quantificador universal em termos da relação $\vdash$:
$\Gamma \vdash \varphi(x) \Rightarrow \Gamma \vdash \forall x \varphi(x)$ se $x \notin VL(\varphi)$ para toda $\varphi \in \Gamma$,
$\Gamma \vdash \forall x \varphi(x) \Rightarrow \Gamma \vdash \varphi(t)$ se $t$ é livre para $x$ em $\varphi$.
As implicações acima seguem diretamente de $(\forall I)$ e $(\forall E)$.

Nosso próximo objetivo é a corretude do sistema de dedução natural para a lógica de predicados. Primeiro estendemos a definição de $\models$.

**Definição 2.8.1** Seja $\Gamma$ um conjunto de fórmulas e suponha que $\{x_{i_1}, x_{i_2}, \ldots\} = \bigcup\{VL(\psi) \mid \psi \in \Gamma \cup \{\sigma\}\}$. Se $\mathbf{a}$ é uma seqüência $(a_1, a_2, \ldots)$ de elementos (repetições permitidas) de $|\mathrm{A}|$, então $\Gamma(\mathbf{a})$ é obtido de $\Gamma$ substituindo simultaneamente em todas as fórmulas de $\Gamma$ os $x_{i_j}$ por $\overline{a_j}$ $(j \geq 1)$ (para $\Gamma = \{\psi\}$ escrevemos $\psi(\mathbf{a})$). Agora definimos

$(i)$ $\mathrm{A} \models \Gamma(\mathbf{a})$ se $\mathrm{A} \models \psi$ para toda $\psi \in \Gamma(\mathbf{a})$
$(ii)$ $\Gamma \models \sigma$ se $\mathrm{A} \models \Gamma(\mathbf{a}) \Rightarrow \mathrm{A} \models \sigma(\mathbf{a})$ para todas $\mathrm{A}, \mathbf{a}$.

No caso em que apenas sentenças forem envolvidas, a definição pode ser simplificada:
$\Gamma \models \sigma$ se $A \models \Gamma \Rightarrow A \models \sigma$ para toda A.
Se $\Gamma = \emptyset$, escrevemos $\models \sigma$.

Podemos parafrasear essa definição da seguinte maneira: $\Gamma \models \sigma$, se para toda estrutura A e todas as escolhas de $\mathbf{a}$, $\sigma(\mathbf{a})$ é verdadeira em A se todas as hipóteses de $\Gamma(\mathbf{a})$ são verdadeiras em A.

Podemos agora formular

**Lema 2.8.2 (Corretude)** $\Gamma \vdash \sigma \Rightarrow \Gamma \models \sigma$.

*Demonstração.* Pela definição de $\Gamma \vdash \sigma$ basta mostrar que para cada derivação com $\Gamma$ como conjunto de hipóteses e com $\sigma$ como conclusão $\Gamma \models \sigma$. Usamos indução sobre $\mathcal{D}$ (cf. 1.5.1 e exercício 2).

Como já demos nossa definição de satisfação em termos de valorações, que evidentemente contém a lógica proposicional como um caso especial, podemos copiar os casos de (1) a derivação com um elemento, (2) as derivações com uma regra proposicional no último passo, do Lema 1.6.1 (favor verifique essa alegação).

Logo temos que tratar as derivações com $(\forall I)$ ou $(\forall E)$ como passo final.

$(\forall I)$ $\dfrac{\begin{array}{c}\mathcal{D}\\ \varphi(x)\end{array}}{\forall x \varphi(x)}$ $\mathcal{D}$ tem suas hipóteses em $\Gamma$ e $x$ não é livre em $\Gamma$.
Hipótese da indução: $\Gamma \models \varphi(x)$, i.e. $A \models \Gamma(\mathbf{a})$
$A \models (\varphi(x))(\mathbf{a})$ para toda A e toda $\mathbf{a}$.

Não significa restrição supor que $x$ é a primeira das variáveis livres envolvidas (por que?). Portanto podemos substituir $x$ por $\overline{a_1}$ em $\varphi$. Ponha $\mathbf{a} = (a_1, \mathbf{a}')$. Agora temos:
para todo $a_1$ e $\mathbf{a}' = (a_2, \ldots)$ $A \models \Gamma(\mathbf{a}') \Rightarrow A \models \varphi(\overline{a_1})(\mathrm{a})$, logo
para toda $\mathbf{a}'$ $A \models \Gamma(\mathbf{a}') \Rightarrow (A \models (\varphi(\overline{a_1}))(\mathbf{a}')$ para todo $a_1$, logo
para toda $\mathbf{a}'$ $A \models \Gamma(\mathbf{a}') \Rightarrow A \models (\forall x \varphi(x))(\mathbf{a}')$.

Isso mostra que $\Gamma \models \forall x \varphi(x)$. (Note que nessa demonstração usamos $\forall x(\sigma \to \tau(x)) \to (\sigma \to \forall x \tau(x))$, onde $x \notin VL(\sigma)$, na metalinguagem. É claro que podemos usar princípios seguros no meta-nível.)

$(\forall E)$ $\dfrac{\begin{array}{c}\mathcal{D}\\ \forall x \varphi(x)\end{array}}{\varphi(t)}$ Hipótese da indução: $\Gamma \models \forall x \varphi(x)$,
i.e. $A \models \Gamma(\mathbf{a}) \Rightarrow A \models (\forall x \varphi(x))(\mathbf{a})$,
para toda $\mathbf{a}$ e A.

Portanto suponha que $A \models \Gamma(\mathbf{a})$, então $A \models \varphi(\overline{b})(\mathbf{a})$ para todo $b \in |A|$. Em particular podemos tomar $t[\overline{\mathbf{a}}/\mathbf{z}]$ para $\overline{b}$, onde abusamos um pouco da notação; como existem um número finito de variáveis $z_1, \ldots, z_n$, precisamos apenas de um número finito de $a_i$'s, e consideramos portanto uma substituição simultânea comum.

$A \models (\varphi[\mathbf{a}/\mathbf{z}])[t[\mathbf{a}/\mathbf{z}]/x]$, daí pelo Lema 2.5.4, $A \models (\varphi[t/x])[\mathbf{a}/\mathbf{z}]$, ou $A \models (\varphi(t))(\mathbf{a})$. $\square$

Tendo estabelecido a corretude de nosso sistema, podemos facilmente obter resultados de não-derivabilidade.

*Exemplos.*

1. $\nvdash \forall x \exists y \varphi \to \exists y \forall x \varphi$.
   Tome $\mathrm{A} = \langle \{0,1\}, \{\langle 0,1\rangle, \langle 1,0\rangle\}\rangle$ (tipo $\langle 2; -; 0\rangle$) e considere
   $\varphi := P(x,y)$, o predicado interpretado em A.
   $\mathrm{A} \models \forall x \exists y P(x,y)$ pois para 0 temos
   $\langle 0,1\rangle \in P$ e para 1 temos $\langle 1,0\rangle \in P$.
   Mas $\mathrm{A} \not\models \exists y \forall x P(x,y)$, pois para 0 temos
   $\langle 0,0\rangle \notin P$ e para 1 temos $\langle 1,1\rangle \notin P$.

2. $\forall x \varphi(x,x), \forall xy(\varphi(x,y) \to \varphi(y,x)) \nvdash \forall xyz(\varphi(x,y) \wedge \varphi(y,z) \to \varphi(x,z))$.
   Considere $\mathrm{B} = \langle \mathbb{R}, P\rangle$ com $P = \{\langle a,b\rangle \mid |a-b| \leq 1\}$.

Embora variáveis e constantes sejam basicamente diferentes, elas têm algumas propriedades em comum. Tanto as constantes como as variáveis livres podem ser introduzidas nas derivações através de $\forall E$, porém apenas as variáveis livres pode ser submetidas à regra $\forall I$, – isto é, variáveis livres podem desaparecer nas derivações por outros meios que não os proposicionais. Segue que uma variável pode tomar o lugar de uma constante numa derivação porém em geral o contrário não é verdadeiro. Tornamos isso mais preciso no que se segue.

**Teorema 2.8.3** *Seja $x$ uma variável que não ocorre em $\Gamma$ ou em $\varphi$.*
(i) $\Gamma \vdash \varphi \Rightarrow \Gamma[x/c] \vdash \varphi[x/c]$.
(ii) *Se $c$ não ocorre em $\Gamma$, então* $\Gamma \vdash \varphi(c) \Rightarrow \Gamma \vdash \forall x \varphi(x)$.

*Demonstração.* (ii) segue imediatamente de (i) por $\forall I$. (i) Indução sobre a derivação de $\Gamma \vdash \varphi$. Deixo ao leitor. □

Observe que o resultado é bastante óbvio, pois trocar $c$ por $x$ é tão inofensivo quanto pintar $c$ de vermelho – a derivação permanece intacta.

**Exercícios**

1. Mostre que:
   (i) $\vdash \forall x(\varphi(x) \to \psi(x)) \to (\forall x \varphi(x) \to \forall x \psi(x))$,
   (ii) $\vdash \forall x \varphi(x) \to \neg \forall x \neg \varphi(x)$,
   (iii) $\vdash \forall x \varphi(x) \to \forall z \varphi(z)$ se $z$ não ocorre em $\varphi(x)$,
   (iv) $\vdash \forall x \forall y \varphi(x,y) \to \forall y \forall x \varphi(x,y)$,
   (v) $\vdash \forall x \forall y \varphi(x,y) \to \forall x \varphi(x,x)$,
   (vi) $\vdash \forall x(\varphi(x) \wedge \psi(x)) \leftrightarrow \forall x \varphi(x) \wedge \forall x \psi(x)$,
   (vii) $\vdash \forall x(\varphi \to \psi(x)) \leftrightarrow (\varphi \to \forall x \psi(x))$.

2. Estenda a definição de derivação para o sistema atual (cf. 1.4.1).

3. Mostre que $(s(t)[\overline{a}/x])^{\mathrm{A}} = (s(\overline{(t[\overline{a}/x])^{\mathrm{A}}})[\overline{a}/x])^{\mathrm{A}}$.

4. Mostre as implicações inversas de 2.8.3.

5. Atribua a cada átomo $P(t_1,\ldots,t_n)$ um símbolo proposicional, denotado por $P$. Agora defina uma tradução † da linguagem da lógica de predicados para a linguage da lógica proposicional da seguinte forma

$P(t_1, \ldots, t_n)^\dagger := P$ e $\perp^\dagger := \perp$
$(\varphi \Box \psi)^\dagger := \varphi^\dagger \Box \psi^\dagger$
$(\neg\psi)^\dagger := \neg\varphi^\dagger$
$(\forall x \varphi)^\dagger := \varphi^\dagger$

Mostre que $\Gamma \vdash \varphi \Rightarrow \Gamma^\dagger \vdash^\dagger \varphi^\dagger$, onde $\vdash^\dagger$ quer dizer "derivável sem usar $(\forall I)$ ou $(\forall E)$" (e a recíproca se verifica?)
Conclua que a lógica de predicados é consistente.
Mostre que a lógica de predicados é conservativa sobre a lógica proposicional (cf. definição 3.1.5).

## 2.9 Adicionando o Quantificador Existencial

Vamos introduzir $\exists x \varphi$ como uma abreviação para $\neg\forall x \neg\varphi$ (o Teorema 2.5.1 nos diz que há uma boa razão para proceder dessa forma). Podemos demonstrar o seguinte:

**Lema 2.9.1**
*(i)* $\varphi(t) \vdash \exists x \varphi(x)$ *(t livre para x em* $\varphi$*)*
*(ii)* $\Gamma, \varphi(x) \vdash \psi \Rightarrow \Gamma, \exists x \varphi(x) \vdash \psi$
*se x não é livre em* $\psi$ *ou em qualquer fórmula de* $\Gamma$.

*Demonstração.* (i)

$$\dfrac{\dfrac{\dfrac{[\forall x \neg\varphi(x)]}{\neg\varphi(t)}\,\forall E \qquad \varphi(t)}{\perp}\rightarrow E}{\neg\forall x \neg\varphi(x)}\rightarrow I$$

logo $\varphi(t) \vdash \exists x \varphi(x)$.

(ii)

$$\dfrac{\dfrac{\neg\forall x\neg\varphi(x) \qquad \dfrac{\dfrac{\dfrac{\dfrac{\begin{matrix}[\varphi(x)]\\ \mathcal{D}\\ \psi\end{matrix} \qquad [\neg\psi]}{\perp}\rightarrow E}{\neg\varphi(x)}\rightarrow I}{\forall x\neg\varphi(x)}\,\forall I}{}}{\perp}\rightarrow E}{\psi}\,\text{RAA}$$

□

*Explicação.* A subderivação no canto superior à esquerda é a derivação dada; suas hipóteses estão em $\Gamma \cup \{\varphi(x)\}$ (apenas $\varphi(x)$ é mostrada). Como $\varphi(x)$ (isto é, todas as ocorrências dessa fórmula) é cancelada e $x$ não ocorre livre em $\Gamma$ ou $\psi$, podemos aplicar $\forall I$. Da derivação concluimos que $\Gamma, \exists x \varphi(x) \vdash \psi$.

Podemos compactar a última derivação em uma regra de eliminação para $\exists$:

$$\dfrac{\exists x\varphi(x) \qquad \begin{matrix}[\varphi(x)]\\ \vdots \\ \psi\end{matrix}}{\psi}\,\exists E$$

com as condições: $x$ não é livre em $\psi$, ou em uma hipótese da subderivação de $\psi$, diferente de $\varphi(x)$.

Isso pode facilmente verificado como correto pois sempre podemos preencher os detalhes ausentes, tal qual mostrado na derivação anterior.

Por (i) temos também uma regra de introdução: $\dfrac{\varphi(t)}{\exists x\varphi(x)}\,\exists I$ para $t$ livre para $x$ em $\varphi$.

*Exemplos de derivações.*

$$\dfrac{\dfrac{\dfrac{[\exists x\varphi(x)]^2 \qquad \dfrac{\dfrac{[\forall x(\varphi(x)\to\psi)]^3}{\varphi(x)\to\psi}\,\forall E \qquad [\varphi(x)]^1}{\psi}\,\to E}{\psi}\,\exists E_1}{\exists x\varphi(x)\to\psi}\,\to I_2}{\forall x(\varphi(x)\to\psi)\to(\exists x\varphi(x)\to\psi)}\,\to I_3 \qquad\qquad x\notin VL(\psi)$$

$$\dfrac{\dfrac{[\exists x(\varphi(x)\vee\psi(x))]^3 \qquad \dfrac{[\varphi(x)\vee\psi(x)]^2 \qquad \dfrac{\dfrac{[\varphi(x)]^1}{\exists x\varphi(x)}}{\exists x\varphi(x)\vee\exists x\psi(x)} \qquad \dfrac{\dfrac{[\psi(x)]^1}{\exists x\psi(x)}}{\exists x\varphi(x)\vee\exists x\psi(x)}}{\exists x\varphi(x)\vee\exists x\psi(x)}\,\vee E_1}{\exists x\varphi(x)\vee\exists x\psi(x)}\,\exists E_2}{\exists x(\varphi(x)\vee\psi(x))\to\exists x\varphi(x)\vee\exists x\psi(x)}\,\to I_3$$

Vamos expor brevemente a abordagem alternativa, ou seja aquela de enriquecer a linguagem.

**Teorema 2.9.2** *Considere a lógica de predicados com a linguagem integral e as regras para todos os conectivos, então* $\vdash \exists x\varphi(x)\leftrightarrow\neg\forall x\neg\varphi(x)$.

*Demonstração.* Semelhante à demonstração do Teorema 1.6.3. $\square$

Agora é hora de enunciar as regras para $\forall$ e $\exists$ com mais precisão. Queremos substituições de termos para algumas ocorrências da variável quantificada em $(\forall E)$ e $(\exists E)$. O exemplo abaixo dá uma motivação para isso.

$$\dfrac{\dfrac{\forall x(x=x)}{x=x}\,\forall E}{\exists y(x=y)}\,\exists I$$

O resultado não seria derivável se pudéssemos apenas fazer substituições para *todas* as ocorrências ao mesmo tempo. Mesmo assim, o resultado é evidentemente verdadeiro.

A formulação apropriada das regras agora é:

$$\forall I \quad \frac{\varphi}{\forall x \varphi} \qquad\qquad \forall E \quad \frac{\forall x \varphi}{\varphi[t/x]}$$

$$\exists I \quad \frac{\varphi[t/x]}{\exists x \varphi} \qquad\qquad \exists E \quad \frac{\exists x \varphi \qquad \begin{array}{c}[\varphi]\\ \vdots \\ \psi\end{array}}{\psi}$$

com as restrições apropriadas.

**Exercícios**

Mostre que:
1. $\vdash \exists x(\varphi(x) \wedge \psi) \leftrightarrow \exists x \varphi(x) \wedge \psi$ se $x \notin VL(\psi)$,
2. $\vdash \forall x(\varphi(x) \vee \psi) \leftrightarrow \forall x \varphi(x) \vee \psi$ se $x \notin VL(\psi)$,
3. $\vdash \forall x \varphi(x) \leftrightarrow \neg\exists x \neg\varphi(x)$,
4. $\vdash \neg\forall x \varphi(x) \leftrightarrow \exists x \neg\varphi(x)$,
5. $\vdash \neg\exists x \varphi(x) \leftrightarrow \forall x \neg\varphi(x)$,
6. $\vdash \exists x(\varphi(x) \to \psi) \leftrightarrow (\forall x \varphi(x) \to \psi)$ se $x \notin VL(\psi)$,
7. $\vdash \exists x(\varphi \to \psi(x)) \leftrightarrow (\varphi \to \exists x \psi(x))$ se $x \notin VL(\varphi)$,
8. $\vdash \exists x \exists y \varphi \leftrightarrow \exists y \exists x \varphi$,
9. $\vdash \exists x \varphi \leftrightarrow \varphi$ se $x \notin VL(\varphi)$.

## 2.10 Dedução Natural e Identidade

Vamos dar regras, correspondendo aos axiomas $I_1 - -I_4$ da seção 2.6.

$$\frac{}{x = x}\,RI_1$$

$$\frac{x = y}{y = x}\,RI_2$$

$$\frac{x = y \quad y = z}{y = z}\,RI_3$$

$$\frac{x_1 = y_1, \ldots, x_n = y_n}{t(x_1, \ldots, x_n) = t(y_1, \ldots, y_n)}\,RI_4$$

$$\frac{x_1 = y_1, \ldots, x_n = y_n \quad \varphi(x_1, \ldots, x_n)}{\varphi(y_1, \ldots, y_n)}\,RI_5$$

onde $y_1, \ldots, y_n$ são livres para $x_1, \ldots, x_n$ em $\varphi$. Note que desejamos permitir substituição da variável $y_i$ $(i \leq n)$ para *alguma* porém não necessariamente todas as ocorrências da variável $x_i$. Podemos expressar isso formulando $RI_4$ nos termos precisos do operador de substituição simultânea:

$$\frac{x_1 = y_1, \ldots, x_n = y_n}{t[x_1, \ldots, x_n/z_1, \ldots, z_n] = t[y_1, \ldots, y_n/z_1, \ldots, z_n]}$$

$$\frac{x_1 = y_1, \ldots, x_n = y_n \quad \varphi[x_1, \ldots, x_n/z_1, \ldots, z_n]}{\varphi[y_1, \ldots, y_n/z_1, \ldots, z_n]}$$

*Exemplo.*

$$\frac{x = y \quad x^2 + y^2 > 12x}{2y^2 > 12x}$$

$$\frac{x = y \quad x^2 + y^2 > 12x}{x^2 + y^2 > 12y}$$

$$\frac{x = y \quad x^2 + y^2 > 12x}{2y^2 > 12y}$$

Os exemplos acima são aplicações legítimas de $RI_4$ que têm três diferentes conclusões.

A regra $RI_1$ não tem hipóteses, o que pode parecer surpreendente, porém certamente não é proibido.

As regras $RI_4$ têm muitas hipóteses, e em conseqüência as árvores de derivação podem parecer um pouco complicadas. Obviamente pode-se obter todos os benefícios de $RI_4$ através de uma regra restrita, permitindo-se apenas uma substituição a cada vez.

**Lema 2.10.1** $\vdash I_i$ *para* $i = 1, 2, 3, 4$.

*Demonstração.* Imediata. $\square$

Podemos enfraquecer um pouco as regras $RI_4$ considerando apenas os termos e as fórmulas mais simples.

**Lema 2.10.2** *Seja* $L$ *do tipo* $\langle r_1, \ldots, r_n; a_1, \ldots, a_m; k\rangle$. *Se as regras*

$$\frac{x_1 = y_1, \ldots, x_{r_i} = y_{r_i} \quad P_1(x_1, \ldots, x_{r_i})}{P_1(y_1, \ldots, y_{r_i})} \ \textit{para todo } i \leq n$$

*e*

$$\frac{x_1 = y_1, \ldots, x_{a_j} = y_{a_j}}{f_j(x_1, \ldots, x_{a_j}) = f_j(y_1, \ldots, y_{a_j})} \ \textit{para todo } j \leq m$$

*são dadas, então as regras* $RI_4$ *são deriváveis.*

*Demonstração.* Consideramos um caso especial. Suponha que $L$ tenha um símbolo binário de predicado e um símbolo unário de função.

(i) Mostramos que $x = y \vdash t(x) = t(y)$ por indução sobre $t$.

(a) $t(x)$ é uma variável ou uma constante. Imediato.

(b) $t(x) = f(s(x))$. Hipótese da indução: $x = y \vdash s(x) = s(y)$

$$\dfrac{\dfrac{\dfrac{\dfrac{[x = y]}{f(x) = f(y)}}{\forall xy(x = y \to f(x) = f(y))}\ \forall I\ 2\times}{s(x) = s(y) \to f(s(x)) = f(s(y))} \qquad \begin{array}{c} x = y \\ \mathcal{D} \\ s(x) = s(y) \end{array}}{f(s(x)) = f(s(y))}$$

Isso mostra que $x = y \vdash f(s(x)) = f(s(y))$.

(ii) Mostramos que $\vec{x} = \vec{y}, \varphi(\vec{x}) \vdash \varphi(\vec{y})$

(a) $\varphi$ é atômica, então $\varphi = P(t,s)$. $t$ e $s$ podem (neste exemplo) conter no máximo uma variável cada. Portanto basta considerar
$x_1 = y_1, x_2 = y_2, P(t(x_1,x_2), s(x_1,x_2)) \vdash P(t(y_1,y_2), s(y_1,y_2))$,
(i.e. $P(t[x_1,x_2/z_1,z_2], \ldots)$.
Agora obtemos, aplicando $\rightarrow E$ duas vezes, de

$$\dfrac{\dfrac{\dfrac{\dfrac{[x_1 = y_1] \quad [x_2 = y_2] \quad [P(x_1,x_2)]}{P(y_1,y_2)}}{x_1 = x_2 \rightarrow (x_2 = y_2 \rightarrow (P(x_1,x_2) \rightarrow P(y_1,y_2)))} \rightarrow I\ 3\times}{\forall x_1 x_2 y_1 y_2 (x_1 = x_2 \rightarrow (x_2 = y_2 \rightarrow (P(x_1,x_2) \rightarrow P(y_1,y_2))))} \forall I}{s(x_1,x_2) = s(y_1,y_2) \rightarrow (t(x_1,x_2) = t(y_1,y_2) \rightarrow (P(s_x,t_x) \rightarrow P(s_y,t_y)))} \forall E$$

e das duas seguintes instâncias de (i)

$$\begin{array}{c} x_1 = y_1 \quad x_2 = y_2 \\ \mathcal{D} \\ s(x_1,x_2) = s(y_1,y_2) \end{array} \quad \text{e} \quad \begin{array}{c} x_1 = y_1 \quad x_2 = y_2 \\ \mathcal{D}' \\ t(x_1,x_2) = t(y_1,y_2) \end{array}$$

o resultado desejado, $(P(x_x,t_x) \rightarrow P(s_y,t_y))$.
Logo $x_1 = y_1, x_2 = y_2 \vdash P(x_x,t_x) \rightarrow P(s_y,t_y)$
onde $s_x = s(x_1,x_2)$, $s_y = s(y_1,y_2)$,
$t_x = t(x_1,x_2)$, $t_y = t(y_1,y_2)$.

(b) $\varphi = \sigma \rightarrow \tau$.
Hipótese da indução: $\vec{x} = \vec{y}, \sigma(\vec{y}) \vdash \sigma(\vec{x})$
$\vec{x} = \vec{y}, \tau(\vec{x}) \vdash \tau(\vec{y})$

$$\dfrac{\dfrac{\dfrac{\sigma(\vec{x}) \rightarrow \tau(\vec{x}) \qquad \begin{array}{c} \vec{x} = \vec{y} \quad [\sigma(\vec{y})] \\ \mathcal{D} \\ \sigma(\vec{x}) \end{array}}{\tau(\vec{x})} \qquad \vec{x} = \vec{y}}{\begin{array}{c} \mathcal{D}' \\ \tau(\vec{y}) \end{array}}}{\sigma(\vec{y}) \rightarrow \tau(\vec{y})}$$

Logo $\vec{x} = \vec{y}, \sigma(\vec{x}) \rightarrow \tau(\vec{x}) \vdash \sigma(\vec{y}) \rightarrow \tau(\vec{y})$.

(c) $\varphi = \sigma \wedge \tau$, deixo ao leitor.

(d) $\varphi = \forall z \psi(z, \vec{x})$
Hipótese da indução: $\vec{x} = \vec{y}, \psi(z,\vec{x}) \vdash \psi(z,\vec{y})$

$$\dfrac{\begin{array}{c} \dfrac{\forall z \psi(z,\vec{x})}{\psi(z,\vec{x})} \quad \vec{x} = \vec{y} \\ \mathcal{D} \\ \psi(z,\vec{y}) \end{array}}{\forall z \psi(z,\vec{y})}$$

Logo $\vec{x} = \vec{y}, \forall z\psi(z, \vec{x}) \vdash \forall z\psi(z, \vec{y})$.
Isso estabelece, por indução, a regra geral. $\square$

**Exercícios**

1. Mostre que $\forall x(x = x), \forall xyz(x = y \wedge z = y \rightarrow x = z) \vdash I_2 \wedge I_3$ (usando apenas a lógica de predicados).

2. Mostre que $\vdash \exists x(t = x)$ para qualquer termo $t$. Explique por que todas as funções em uma estrutura são totais (i.e. definidas para todos os argumentos); que significa $0^{-1}$?

3. Mostre que $\vdash \forall z(z = x \rightarrow z = y) \rightarrow x = y$.

4. Mostre que $\vdash \forall xyz(x \neq y \rightarrow x \neq z \vee y \neq z)$.

5. Mostre que na linguagem da identidade, $I_1, I_2, I_3 \vdash I_4$.

6. Mostre que $\forall x(x = a \vee x = b \vee x = c) \vdash \forall x\varphi(x) \leftrightarrow (\varphi(a) \vee \varphi(b) \vee \varphi(c))$, onde $a, b, c$ são constantes.

7. Mostre que:

   (i) $\forall xy(f(x) = f(y) \rightarrow x = y), \forall xy(g(x) = g(y) \rightarrow x = y) \vdash \forall xy(f(g(x)) = f(g(y)) \rightarrow x = y)$,

   (ii) $\forall y\exists x(f(x) = y), \forall y\exists x(g(x) = y) \vdash \forall y\exists x(f(g(x)) = y)$.

   Que propriedades são expressas por esse exercício?

8. Demonstre o seguinte *Princípio da Dualidade* para a geometria projetiva (cf. definição 2.7.5): Se $\Gamma \vdash \varphi$ então temos também $\Gamma \vdash \varphi^d$, onde $\Gamma$ é o conjunto de axiomas da geometria projetiva e $\varphi^d$ é obtida de $\varphi$ substituindo cada átomo $xIy$ por $yIx$. (Sugestão: verifique o efeito da tradução $d$ sobre a derivação de $\varphi$ a partir de $\Gamma$.

# Capítulo 3

# Completude e Aplicações

## 3.1 O Teorema da Completude

Tal qual no caso da lógica proposicional mostraremos que 'derivabilidade' e 'conseqüência semântica' coincidem. Faremos bastante coisa antes de chegar no teorema. Embora a demonstração do teorema da completude não seja mais difícil que, digamos, algumas demonstrações em análise, recomendaríamos ao leitor que fizesse uma leitura do enunciado do teorema e que saltasse a demonstração na primeira leitura, retornando a ela mais tarde. É mais instrutivo ir às aplicações e isso provavelmente dará ao leitor um melhor sentimento para o assunto.

A principal ferramenta neste capítulo é o

**Lema 3.1.1 (Lema da Existência de Modelo)** *Se $\Gamma$ é um conjunto consistente de sentenças, então $\Gamma$ tem um modelo.*

Uma versão mais refinada é

**Lema 3.1.2** *Suponha que $L$ tenha cardinalidade $\kappa$. Se $\Gamma$ é um conjunto consistente de sentenças, então $\Gamma$ tem um modelo de cardinalidade $\leq \kappa$.*

De 3.1.1 imediatamente deduzimos o teorema de Gödel

**Teorema 3.1.3 (Teorema da Completude)** $\Gamma \vdash \varphi \Leftrightarrow \Gamma \models \varphi$.

Passaremos agora por todos os passos da demonstração do teorema da completude. Nesta seção consideraremos sentenças, a menos que mencionemos especificamente fórmulas não-fechadas. Além do mais, '$\vdash$' representará 'derivabilidade na lógica de predicados com identidade'.

Tal qual no caso da lógica proposicional temos que construir um modelo e a única coisa que temos é nossa teoria consistente. Essa construção é uma espécie de truque do Barão de Münchhausen; temos que nos sacar (na verdade, sacar um modelo) de uma montanha de sintaxe e de regras de prova. A idéia mais plausível é formar um universo a partir de termos fechados e definir relações como os conjuntos de (uplas de) termos nos átomos da teoria. Há basicamente duas coisas que temos que cuidar: (i) se a teoria nos diz que $\exists x\varphi(x)$, então o modelo tem que fazer com que $\exists x\varphi(x)$ seja verdadeira, e portanto é que preciso exibir um elemento (que nesse caso é um termo fechado $t$) tal que $\varphi(t)$ seja verdadeira.

Isso significa que a teoria tem que provar $\varphi(t)$ para um termo fechado apropriado $t$. Esse problema é resolvido nas chamadas teorias de Henkin. (ii) Um modelo tem que decidir sentenças, i.e. ele tem que dizer se $\sigma$ ou $\neg\sigma$ se verificam, para cada sentença $\sigma$. Tal qual em lógica proposicional, isso é tratado pelas teorias consistentes maximais.

**Definição 3.1.4** (i) Uma *teoria* $T$ é uma coleção de sentenças com a propriedade $T \vdash$
$varphi \Rightarrow \varphi \in T$ (uma teoria é *fechada sob derivabilidade*).

(ii) Um conjunto $\Gamma = \{\varphi \mid T \vdash \varphi\}$ é chamado de um *conjunto de axiomas* da teoria $T$. Os elementos de $T$ são chamados *axiomas*.

(iii) $T$ é chamado de uma *teoria de Henkin* se para cada sentença $\exists x\varphi(x)$ existe uma constante $c$ tal que $\exists x\varphi(x) \to \varphi(c) \in T$ (tal constante $c$ é chamada de uma *testemunha* para $\exists x\varphi(x)$).

Note que $T = \{\sigma \mid \Gamma \vdash \sigma\}$ é uma teoria. Pois, se $T \vdash \sigma$, então $\sigma_1, \ldots, \sigma_k \vdash \varphi$ para uma certa $\varphi_i$ com $\Gamma \vdash \sigma_i$.

figura

**Definição 3.1.5** Sejam $T$ e $T'$ teorias nas linguagens $L$ e $L'$.

(i) $T'$ é *extensão* de $T$ se $T \subseteq T'$,

(ii) $T'$ é uma *extensão conservativa* de $T$ se $T' \cap L = T$ (i.e. todos os teoremas de $T'$ na linguagem $L$ já são teoremas de $T$).

Exemplo de uma extensão conservativa: Considere uma lógica proposicional $P'$ na linguagem $L$ com $\to$, $\wedge$, $\bot$, $\leftrightarrow$, ./ Então o exercício 2, seção 1.6, nos diz que $P'$ é conservativa sobre $P$.

Nossa primeira tarefa é a construção de *extensões de Henkin* de uma dada teoria $T$, isto é: extensões de $T$ que sejam teorias de Henkin.

**Definição 3.1.6** Seja $T$ uma teoria com linguagem $L$. A linguagem $L^*$ é obtida a partir de $L$ pela adição de uma constante $c_\varphi$ para cada sentença da forma $\exists x\varphi(x)$, uma constante $c_\varphi$. $T^*$ é a teoria com o conjunto de axiomas

$$T \cup \{\exists x\varphi(x) \to \varphi(c_\varphi) \mid \exists x\varphi(x) \text{ é fechada, com testemunha } c_\varphi\}.$$

**Lema 3.1.7** *$T^*$ é conservativa sobre $T$.*

*Demonstração.* (a) Seja $\exists x\varphi(x) \to \varphi(c)$ um dos novos axiomas. Suponha que $\Gamma, \exists x\varphi(x) \to \varphi(c) \vdash \psi$, onde $\psi$ não contém $c$ e $\Gamma$ é um conjunto de sentenças, nenhuma das quais contém a constante $c$. Vamos mostrar que $\Gamma \vdash \psi$ em um certo número de passos.

1. $\Gamma \vdash \exists x\varphi(x) \to \varphi(c)) \to \psi$,

2. $\Gamma \vdash \exists x\varphi(x) \to \varphi(y)) \to \psi$, onde $y$ é uma variável que não ocorre na derivação associada. 2 segue de 1 pelo Teorema 2.8.3.

3. $\Gamma \vdash \forall y((\exists x\varphi(x) \to \varphi(y)) \to \psi)$. Essa aplicação de $(\forall I)$ está correta, pois $c$ não ocorria em $\Gamma$.

4. $\Gamma \vdash \exists y(\exists x\varphi(x) \to \varphi(y)) \to \psi$, (cf. exemplo da seção 2.9).

5. $\Gamma \vdash (\exists x\varphi(x) \to \exists y\varphi(y)) \to \psi$, (seção 2.9, exercício 7).

6. $\vdash \exists x\varphi(x) \to \exists y\varphi(y)$.

7. $\Gamma \vdash \psi$, (de 5.6).

(b) Suponha que $T^* \vdash \psi$ para uma $\psi \in L$. Pela definição de derivabilidade $T \cup \{\sigma_1, \ldots, \sigma_n\} \vdash \psi$, onde $\sigma_i$ são os novos axiomas da forma $\exists x\varphi(x) \to \varphi(c)$. Vamos mostrar que $T \vdash \psi$ por indução sobre $n$. Para $n = 0$ estamos resolvidos. Suponha que $T \cup \{\sigma_1, \ldots, \sigma_{n+1}\} \vdash \psi$. Faça $\Gamma' = T \cup \{\sigma_1, \ldots, \sigma_n\}$, então $T', \sigma_{n+1} \vdash \psi$ e podemos aplicar o item (a). Daí, $T \cup \{\sigma_1, \ldots, \sigma_n\} \vdash \psi$. Agora, pela hipótese da indução, $T \vdash \psi$. □

Embora tenhamos adicionado um número de testemumhas a $T$, não há evidência de que $T^*$ seja uma teoria de Henkin, pois ao enriquecer a linguagem nós também adicionamos novos enunciados existenciais $\exists x\tau(x)$ que podem não ter testemunhas. De modo a contornar essa dificuldade iteramos o processo acima um número contável de vezes.

**Lema 3.1.8** *Defina* $T_0 := T$*;* $T_{n+1} := (T_n)^*$*;* $T_\omega := \bigcup\{T_n \mid n \geq 0\}$*. Então* $T_\omega$ *é uma teoria de Henkin e é conservativa sobre* $T$*.*

*Demonstração.* Chamemos de $L_n$ (resp. $L_\omega$) a linguagem de $T_n$ (resp. $T_\omega$).

(i) $T_n$ é conservativa sobre $T$. Indução sobre $n$.

(ii) $T_\omega$ é uma teoria. Suponha que $T_\omega \vdash \sigma$, então $\varphi_0, \ldots, \varphi_n \vdash \sigma$ para certas $\varphi_0, \ldots, \varphi_n \in T_\omega$. Para cada $i \leq n$ $\varphi_i \in T_{m_i}$ para algum $m_i$. Seja $m = \max\{m_i \mid i \leq n\}$. Como $T_k \subseteq T_{k+1}$ para todo $k$, temos que $T_{m_i} \subseteq T_m$ $(i \leq n)$. Por conseguinte $T_m \vdash \sigma$. $T_m$ é (por definição) uma teoria, logo $\sigma \in T_m \subseteq T_\omega$.

(iii) $T_\omega$ é uma teoria de Henkin. Seja $\exists x\varphi(x) \in L_\omega$, então $\exists x\varphi(x) \in L_n$ para algum $n$. Por definição $\exists x\varphi(x) \to \varphi(c) \in T_{n+1}$ para um certo $c$. Logo $\exists x\varphi(x) \to \varphi(c) \in T_\omega$.

(iv) $T_\omega$ é conservativa sobre $T$. Observe que $T_\omega \vdash \sigma$ se $T_n \vdash \sigma$ para algum $n$ e aplique (i). □

Como um corolário obtemos: $T_\omega$ é consistente se $T$ também o é. Pois suponha que $T_\omega$ seja inconsistente, então $T_\omega \vdash \bot$. Como $T_\omega$ é conservativa sobre $T$ (e $\bot \in L$) $T \vdash \bot$. Contradição.

Nosso próximo passo é estender $T_\omega$ tanto quanto possível, tal como fizemos na lógica proposicional (1.5.7). Enunciamos um princípio geral.

**Lema 3.1.9 (Lindenbaum)** *Cada teoria consistente está contida em uma teoria maximamente consistente.*

*Demonstração.* Fazemos uma aplicação direta do *Lema de Zorn*. Seja $T$ consistente. Considere o conjunto $A$ de todas as extensões consistentes $T'$ de $T$, parcialmente ordenadas por inclusão. Alegação: $A$ tem um elemento maximal.

1. Cada cadeia em $A$ tem um limitante superior. Seja $\{T_i \mid i \in I\}$ uma cadeia. Então $T' = \bigcup T_i$ é uma extensão consistente de $T$ contendo todos os $T_i$'s (Exercício 2). Logo $T'$ é um limitante superior.

2. Por conseguinte $A$ tem um elemento maximal $T_m$ (lema de Zorn).

3. $T_m$ é uma extensão maximamente consistente de $T$. Apenas temos que demonstrar que: se $T_m \subseteq T'$ e $T' \in A$, então $T_m = T'$. Mas isso é trivial pois $T_m$ é maximal no sentido de $\subseteq$. Conclusão: $T$ está contida na teoria maximamente consistente $T_m$. □

Note que em geral $T$ tem muitas extensões maximamente consistentes. A existência acima está longe de ser única (na verdade a demonstração de sua existência usa essencialmente o axioma da escolha). Note, entretanto, que se a linguagem é contável, pode-se reproduzir a demonstração de 1.5.7 e dispensar o Lema de Zorn.

Agora combinamos a construção de uma extensão de Henkin com uma extensão maximamente consistente. Felizmente a propriedade de ser uma teoria de Henkin é preservada sob a operação de se tomar uma extensão maximamente consistente. Pois, a linguagem permanece fixa, daí se para um enunciado existencial $\exists x\varphi(x)$ existe uma testemunha $c$ tal que $\exists x\varphi(x) \to \varphi(c) \in T$, então trivialmente, $\exists x\varphi(x) \to \varphi(c) \in T_m$. Portanto

**Lema 3.1.10** *Uma extensão de uma teoria de Henkin com a mesma linguagem é novamente uma teoria de Henkin.*

Agora chegamos à demonstração de nosso principal resultado.

**Lema 3.1.11 (Lema da Existência de Modelo)** *Se $\Gamma$ é consistente, então $\Gamma$ tem um modelo*

*Demonstração.* Seja $T = \{\sigma \mid \Gamma \vdash \sigma\}$ a teoria dada por $\Gamma$. Qualquer modelo de $T$ é, obviamente, um modelo de $\Gamma$.

Seja $T_m$ uma extensão de Henkin maximamente consistente de $T$ (que existe pelos lemas precedentes), com linguagem $L_m$.

Construiremos um modelo de $T_m$ usando a própria $T_m$. Nesse ponto o leitor deveria se dar conta que uma linguagem é, afinal de contas, um conjunto, ou seja um conjunto de cadeias de símbolos. Portanto, exploraremos esse conjunto para construir o universo de um modelo apropriado.

1. $A = \{t \in L_m \mid t \text{ é fechado}\}$.

2. Para cada símbolo de função $\overline{f}$ definimos uma função $\hat{f} : A^k \to A$ por $\hat{f}(t_1, \ldots, t_k) := f(t_1, \ldots, t_k)$.

3. Para cada símbolo de predicado $\overline{P}$ definimos uma relação $\hat{P} \subseteq A^p$ por $\langle t_1, \ldots, t_p\rangle \in \hat{P} \Leftrightarrow T_m \vdash P(t(t_1, \ldots, t_p)$.

4. Para cada símbolo de constante $c$ definimos uma constante $\hat{c} := c$.

Embora possa parecer que criamos o modelo desejado, temos que melhorar o resultado, porque '=' não é interpretado como a real igualdade. Podemos apenas afirmar que

(a) A relação $t \sim s$ definida por $T_m \vdash t = s$ para $t, s \in A$ é uma relação de equivalência. Pelo lema 2.10.1, $I_1$, $I_2$, $I_3$ são teoremas de $T_m$, logo $T_m \vdash \forall x(x = x)$, e portanto (por $(\forall E)$ $T_m \vdash t = t$, ou $t \sim t$. Simetria e transitividade seguem da mesma maneira.

(b) $t_i \sim s_i$ $(i \leq p)$ e $\langle t_1, \ldots, t_p\rangle \hat{P} \Rightarrow \langle s_1, \ldots, s_p\rangle \in \hat{P}$.
$t_i \sim s_i (i \leq k) \Rightarrow \hat{f}(t_1, \ldots, t_k) \sim \hat{f}(s_1, \ldots, s_k)$ para todos os símbolos $P$ e $f$.

A demonstração é simples: use $T_m \vdash I_4$ (Lema 2.10.1).

Uma vez que temos uma relação de equivalência, que, além do mais, é uma congruência com respeito às relações e funções básicas, é natural introduzir a estrutura quociente.

Denotemos a classe de equivalência de $t$ sob $\sim$ por $[t]$.

Defina $\mathfrak{A} := \langle A/\sim, \tilde{P}_1, \ldots, \tilde{P}_n, \tilde{f}_1, \ldots, \tilde{f}_m, \{\overline{c}_i \mid i \in I\}\rangle$, onde
$\tilde{P}_i := \{\langle [t_1], \ldots, [t_{r_i}]\rangle \mid \langle t_1, \ldots, t_{r_i}\rangle \in \hat{P}_i\}$
$\tilde{f}_j([t_1], \ldots, [t_{a_j}]) = [\hat{f}_j(t_1, \ldots, t_{a_j})]$
$\tilde{c}_i := [\hat{c}_i]$.

É preciso mostrar que as relações e as funções em $A/\sim$ estão bem-definidas, mas isso já é garantido pelo item (b) acima.

Termos fechados levam a uma espécie de vida dupla. Por um lado eles são objetos sintáticos, por outro lado eles são o material a partir do qual os elementos do universo são feitos. As duas coisas estão relacionadas por $t^{\mathfrak{A}} = [t]$. Isso é demonstrado por indução sobre $t$.

(i) $t = c$, então $t^{\mathfrak{A}} = \overline{c} = [\hat{c}] = [t]$,

(ii) $t = f(t_1, \ldots, t_k)$, então $t^{\mathfrak{A}} = \tilde{f}(t^{\mathfrak{A}_1}, \ldots, t^{\mathfrak{A}_k}) \overset{h.i.}{=} \tilde{f}([t_1], \ldots, [t_k])$
$= [\hat{f}(t_1, \ldots, t_k)] = [f(t_1, \ldots, t_k)]$.

Além disso temos que $\mathfrak{A} \models \varphi(t) \Leftrightarrow \mathfrak{A} \models \varphi(\overline{[t]})$, pelo que foi dito acima e pelo Exercício 6 da seção 2.4.

Alegação. $\mathfrak{A} \models \varphi(t) \Leftrightarrow T_m \vdash \varphi(t)$ para todas as sentenças na linguagem $L_m$ de $T_m$ que, aliás, é também $L(\mathfrak{A})$, pois cada elemento de $A/sim$ tem um nome em $L_m$. Demonstramos a alegação por indução sobre $\varphi$.

(i) $\varphi$ é atômica. $\mathfrak{A} \models P(t_1, \ldots, t_p) \leftrightarrow \langle t_1^{\mathfrak{A}}, \ldots, t_p^{\mathfrak{A}}\rangle \in \tilde{P} \Leftrightarrow \langle [t_1, \ldots, [t_p]\rangle \in \tilde{P} \Leftrightarrow \langle t_1, \ldots, t_p\rangle \in \hat{P} \Leftrightarrow T_m \vdash P(t_1, \ldots, t_p)$. O caso $\varphi = \bot$ é trivial.

(ii) $\varphi = \sigma \wedge \tau$. Trivial.

(iii) $\varphi = \sigma \to \tau$. Lembramos que, pelo lema 1.6.9, $T_m \vdash \sigma \to \tau \Leftrightarrow (T_m \vdash \sigma \Rightarrow T_m \vdash \tau)$. Note que podemos copiar esse resultado, pois sua demonstração usa apenas lógica proposicional, e portanto permanece correta em lógica de predicados.

$$\mathfrak{A} \models \varphi \to \tau \Leftrightarrow (\mathfrak{A} \models \sigma \Rightarrow \mathfrak{A} \models \tau) \overset{h.i.}{\Leftrightarrow} (T_m \vdash \sigma \Rightarrow T_m \vdash \tau) \Leftrightarrow T_m \vdash \sigma \to \tau.$$

(iv) $\varphi = \forall x\psi(x)$. $\mathfrak{A} \models \forall x\psi(x) \Leftrightarrow \mathfrak{A} \not\models \exists x\neg\psi(x) \Leftrightarrow \mathfrak{A} \not\models \neg\psi(\overline{a})$, para todo $a \in |\mathfrak{A}| \Leftrightarrow$ para todo $a \in |\mathfrak{A}|$ $(\mathfrak{A} \models \psi(\overline{a}))$. Assumindo que $\mathfrak{A} \models \forall x\psi(x)$, obtemos, em particular, que $\mathfrak{A} \models \psi(c)$ para a testemunha $c$ correspondente a $\exists x\neg\psi(x)$. Pela hipótese da indução, $T_m \vdash \psi(c)$. $T_m \vdash \exists x\neg\psi(x) \to \neg\psi(c)$, logo $T_m \vdash \psi(c) \to \neg\exists x\neg\psi(x)$. Daí, $T_m \vdash \forall x\psi(x)$.

Reciprocamente: $T_m \vdash \forall x\psi(x) \Rightarrow T_m \vdash \psi(t)$, portanto $T_m \vdash \psi(t)$ para todo termo fechado $t$, e daí, pela hipótese da indução, $\mathrm{A} \models \psi(t)$ para todo termo fechado $t$. Daí, $\mathrm{A} \models \forall x\psi(x)$.

Agora vemos que A é um modelo de $\Gamma$, pois $\Gamma \subseteq T_m$. □

O modelo construído acima é conhecido por vários nomes, às vezes chamado de *modelo canônico* ou *modelo de termos (fechados)*. Em programação em lógica o conjunto dos termos fechados de qualquer linguagem é chamado de *universo de Herbrand* ou *domínio de Herbrand*, e o modelo canônico é chamado de *modelo de Herbrand*.

Para termos uma estimativa da cardinalidade do modelo temos que calcular o número de termos fechados em $L_m$. Como não mudamos de linguagem ao passar de $T_\omega$ para $T_m$, podemos olhar para a linguagem $L_\omega$. Indicaremos como obter as cardinalidades desejadas, dado o alfabeto da linguagem original $L$. Usaremos livremente o axioma da escolha, em particular na forma das leis de absorção (i.e. $\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda)$ para cardinais infinitos). Digamos que $L$ tem tipo $\langle r_1, \ldots, r_n\rangle; a_1, \ldots, a_m\rangle; \kappa\rangle$.

1. Defina

$$\begin{array}{lcl} TERM_0 & := & \{c_i \mid i \in I\} \cup \{x_j \mid j \in N\} \\ TERM_{n+1} & := & TERM_n \cup \{f_j(t_1, \ldots, t_{a_j}) \mid j \leq m, \\ & & t_k \in TERM_n \text{ para } k \leq a_j\}. \end{array}$$

   Então $TERM = \bigcup\{TERM_n \mid n \in N\}$ (Exercício 5)

   $|TERM_0| = \max(\kappa, \aleph_0) = \mu$.

   Suponha que $|TERM_n| = \mu$. Então
   $|\{f_j(t_1, \ldots, t_{a_j}) \mid t_1, \ldots, t_{a_j} \in TERM_n\}| = |TERM_n|^{a_j} = \mu^{a_j} = \mu$. Logo
   $|TERM_{n+1}| = \mu + \mu + \ldots + \mu$ $(m+1$ vezes$) = \mu$.

   Finalmente $|TERM| = \sum_{n \in N} |TERM_n| = \aleph_0 \cdot \mu = \mu$.

2. Defina

$$\begin{array}{lcl} FORM_0 & := & \{P_i(t_1, \ldots, t_{r_i}) \mid i \leq n, t_k \in TERM\} \cup \{\bot\} \\ FORM_{n+1} & := & FORM_n \cup \{\varphi \Box \psi \mid \Box \in \{\wedge, \rightarrow\}, \varphi, \psi \in FORM_n\} \\ & & \cup \{\forall x_i \varphi \mid i \in N, \varphi \in FORM_n\}. \end{array}$$

   Então $FORM = \bigcup\{FORM_n \mid n \in N\}$ (Exercício 5)

   Como no item 1. mostra-se que $|FORM| = \mu$.

3. O conjunto de sentenças da forma $\exists x\varphi(x)$ tem cardinalidade $\mu$. Ela é trivialmente $\leq \mu$. Considere $A = \{\exists x(x = c_i) \mid i \in I\}$. Claramente $|A| = \kappa \cdot \aleph_0 = \mu$. Daí, a cardinalidade dos enunciados existenciais é $\mu$.

4. $L_1$ tem os símbolos de constante de $L$, mais as testemunhas. Pelo item 3. a cardinalidade do conjunto de símbolos de constante é $\mu$. Usando 1. e 2. chegamos à conclusão que $L_0$ tem $\mu$ termos e $\mu$ fórmulas. Por indução sobre $n$ cada $L_n$ tem $\mu$ termos e $\mu$ fórmulas. Por conseguinte $L_\omega$ tem $\aleph_0 \cdot \mu = \mu$ termos e fórmulas. $L_\omega$ também é a linguagem de $T_m$.

5. $L_\omega$ tem no máximo $\mu$ termos fechados. Como $L_1$ tem $\mu$ testemunhas, $L_\omega$ tem no mínimo $\mu$, e portanto exatamente $\mu$ termos fechados.

6. O conjunto dos termos fechados tem $\leq \mu$ classes de equivalência sob $\sim$, logo $|\mathrm{A}| \leq \mu$.

Tudo isso se soma para chegar à versão fortalecida do Lema da Existência de Modelo:

**Lema 3.1.12** *$\Gamma$ é consistente $\leftrightarrow$ $\Gamma$ tem um modelo de cardinalidade no máximo a cardinalidade da linguagem.*

Note os seguintes fatos:

– Se $L$ tem um número infinito de constantes, então $L$ é contável.

– Se $L$ tem $\kappa \geq \aleph_0$ constantes, então $|L| = \kappa$.

O teorema da completude para a lógica de predicados levanta a mesma questão que o teorema da completude para a lógica proposicional: podemos efetivamente encontrar uma derivação de $\varphi$ se $\varphi$ é verdadeira? O problema é que não temos muito no que nos apoiar; $\varphi$ é verdadeira em todas as estruturas (do tipo de similaridade apropriado). Muito embora (no caso de uma linguagem contável) podemos nos restringir a estruturas contáveis, o fato de que $\varphi$ é verdadeira em todas as estruturas não dá a informação combinatória necessária para construir uma derivação de $\varphi$. O problema nesse estágio está além das nossas possibilidades. Um tratamento do problema está na alçada da teoria da prova; o cálculo de seqüentes de Gentzen ou o método do tableau são mais apropriados para a busca de derivações que a dedução natural.

No caso da lógica de predicados existem certos melhoramentos em cima do teorema da completude. Pode-se, por exemplo, perguntar o quão complicado é o modelo que construimos no lema da existência de modelo. O ambiente apropriado para essas questões vai ser encontrado na teoria da recursão. Podemos, entretanto, dar uma rápida olhada num caso simples.

Seja $T$ uma teoria *decidível* com uma linguagem contável, i.e. temos um método efetivo de testar pertinência (ou, o que resulta na mesma coisa, podemos testar se $\Gamma \vdash \varphi$ para um conjunto de axiomas de $T$). Considere a teoria de Henkin introduzida em 3.1.8; $\sigma \in T_\omega$ se $\sigma \in T_n$ para um certo $n$. Esse número $n$ pode ser obtido de $\sigma$ por inspeção das testemunhas ocorrendo em $\sigma$. Das testemunhas podemos também determinar quais axiomas da forma $\exists x \varphi(x) \rightarrow \varphi(c)$ estão envolvidos. Seja $\{\tau_1, \ldots, \tau_n\}$ o conjunto de axiomas necessários para a derivação de $\sigma$, então $T \cup \{\tau_1, \ldots, \tau_n\} \vdash \sigma$. Pelas regras da lógica isso se reduz a $T \vdash \tau_1 \wedge \ldots \wedge \tau_n \rightarrow \sigma$. Como as constantes $c_i$ são novas com respeito a $T$, isso é equivalente a $T \vdash \forall z_1 \ldots z_k(\tau_n' \rightarrow \sigma')$ para variáveis apropriadas $z_1, \ldots, z_k$, onde $\tau_1', \ldots, \tau_n', \sigma'$ são obtidas por substituição. Portanto vemos que $\sigma \in T_\omega$ decidível. O próximo passo é a formação de uma extensão maximal $T_m$.

Seja $\varphi_0, \varphi_1, \varphi_2, \ldots$ uma enumeração de todas as sentenças de $T_\omega$. Adicionamos sentenças a $T_\omega$ em etapas.

figura pagina 112

$$\text{etapa } 0: \quad T_0 = \begin{cases} T_\omega \cup \{\varphi_0\} & \text{se } T \cup \{\varphi_0\} \text{ é consistente,} \\ T_\omega \cup \{\neg\varphi_0\} & \text{caso contrário.} \end{cases}$$

$$\text{etapa } n+1: \quad T_{n+1} = \begin{cases} T_n \cup \{\varphi_{n+1}\} & \text{se } T_n \cup \{\varphi_{n+1}\} \text{ é consistente,} \\ T_n \cup \{\neg\varphi_{n+1}\} & \text{caso contrário.} \end{cases}$$

$T^\circ = \bigcup T_n$ ($T^\circ$ é dada por um caminho infinito apropriado na árvore). É facilmente verificado que $T^\circ$ é maximamente consistente. Além do mais, $T^\circ$ é decidível. Para testar $\varphi_n \in T^\circ$ temos que testar se $\varphi_n \in T_n$ ou $T_{n-1} \cup \{\varphi_n\} \vdash \bot$, que é decidível. Logo $T^\circ$ é decidível.

O modelo $\mathfrak{A}$ construído em 3.1.11 é portanto decidível também no seguinte sentido: as operações e relações de $\mathfrak{A}$ são decidíveis, o que significa que $\langle [t_1], \ldots, [t_p] \rangle \in \tilde{P}$ e $\tilde{f}([t_1], \ldots, [t_k]) = [t]$ são decidíveis.

Resumindo, dizemos que uma teoria consistente decidível tem um modelo decidível (isso pode ser dito de modo mais preciso substituindo 'decidível' por 'recursivo').

**Exercícios**

1. Considere a linguagem dos grupos. $T = \{\sigma \mid \mathfrak{A} \models \sigma\}$, onde $\mathfrak{A}$ é um grupo fixo não-trivial. Mostre que $T$ não é uma teoria de Henkin.

2. Seja $\{T_i \mid i \in I\}$ um conjunto de teorias, linearmente ordenadas por inclusão. Mostre que $T = \bigcup\{T_i \mid i \in I\}$ é uma teoria que estende cada $T_i$. Se cada $T_i$ é consistente, então $T$ é consistente.

3. Mostre que $\lambda_n \vdash \sigma \Leftrightarrow \sigma$ se verifica em todos os modelos com pelo menos $n$ elementos. $\mu_n \vdash \sigma \Leftrightarrow \sigma$ se verifica em todos os elementos com no máximo $n$ elementos. $\lambda_n \wedge \mu_n \vdash \sigma \Leftrightarrow \sigma$ se verifica em todos os modelos com exatamente $n$ elementos, $\{\lambda_n \mid n \in \mathbb{N}\} \vdash \sigma \Leftrightarrow \sigma$ se verifica em todos os modelos infinitos, (para ver uma definição de $\lambda_n$, $\mu_n$, veja seção 2.7).

4. Mostre que $T = \{\sigma \mid \mu_2 \vdash \sigma\} \cup \{c_1 \neq c_2\}$ em uma linguagem com $=$ e dois símbolos de constante $c_1$, $c_2$, é uma teoria de Henkin.

5. Mostre que $TERM = \bigcup\{TERM_n \mid n \in \mathbb{N}\}$, $FORM = \bigcup\{FORM_n \mid n \in \mathbb{N}\}$ (cf. 1.1.5).

## 3.2 Compaccidade e Skolem–Löwenheim

A menos que se diga o contrário, consideramos sentenças nesta seção. Do Lema da Existência de Modelo obtemos o seguinte:

**Teorema 3.2.1 (Teorema da Compaccidade)** *$\Gamma$ tem um modelo $\Leftrightarrow$ cada subconjunto finito $\Delta$ de $\Gamma$ tem um modelo.*

Uma formulação equivalente é:

*$\Gamma$ não tem modelo $\Leftrightarrow$ algum $\Delta$ finito tal que $\Delta \subseteq \Gamma$ não tem modelo*

*Demonstração.* Consideramos a segunda versão.
$\Leftarrow$: Trivial.
$\Rightarrow$: Suponha que $\Gamma$ não tem modelo, então pelo Lema da Existência de Modelo $\Gamma$ é inconsistente, i.e. $\Gamma \vdash \bot$. Por conseguinte existem $\sigma_1, \ldots, \sigma_n \in \Gamma$ tais que $\sigma_1, \ldots, \sigma_n \vdash \bot$. Isso mostra que $\Delta = \{\sigma_1, \ldots, \sigma_n\}$ não tem modelo. $\square$

Vamos introduzir um pouco de notação: $\mathrm{Mod}(\Gamma) = \{\mathrm{A} \mid \mathrm{A} \models \sigma$ para toda $\sigma \in \Gamma\}$. Por conveniência escreveremos com freqüência $\mathrm{A} \models \Gamma$ para $\mathrm{A} \in \mathrm{Mod}(\Gamma)$. Escrevemos $\mathrm{Mod}(\varphi_1, \ldots, \varphi_n)$ ao invés de $\mathrm{Mod}(\{\varphi_1, \ldots, \varphi_n\})$.

Em geral $\mathrm{Mod}(\Gamma)$ não é um conjunto (no sentido técnico de teoria dos conjuntos: $\mathrm{Mod}(\Gamma)$ é na maioria das vezes uma classe própria). Não nos preocuparemos com isso pois a notação é usada apenas como uma abreviação.

Reciprocamente, seja $\mathcal{K}$ uma classe de estruturas (fixamos o tipo de similaridade), então $\mathrm{Th}(\mathcal{K}) = \{\sigma \mid \mathrm{A} \models \sigma$ para toda $\mathrm{A} \in \mathcal{K}\}$. Chamamos $\mathrm{Th}(\mathcal{K})$ de *teoria de* $\mathcal{K}$.

Adotamos a convenção (já usada na seção 2.7) de não incluir os axiomas de identidade em um conjunto $\Gamma$; eles serão sempre satisfeitos.

*Exemplos.*

1. $\mathrm{Mod}(\forall xy(x \leq y \wedge y \leq x \leftrightarrow x = y), \forall xyz(x \leq y \wedge y \leq z \rightarrow x \leq z))$ é a classe dos conjuntos parcialmente ordenados.

2. Seja $\mathcal{G}$ a classe de todos os grupos. $\mathrm{Th}(\mathcal{G})$ é a teoria dos grupos.

Podemos considerar o conjunto dos inteiros com a estrutura de grupo aditivo usual, mas também com a estrutura de anel, portanto existem duas estruturas A e B, das quais a primeira é num certo sentido uma parte da segunda (teoria das categorias usa um funtor esquecimento para expressar isso). Dizemos que A é um *reduto* de B, ou que B é uma *expansão* de A.

Em geral

**Definição 3.2.2** A é um *reduto* de B (B uma *expansão* de A) se $|\mathrm{A}| = |\mathrm{B}|$ e além do mais todas as relações, funções e constantes de A ocorrem também como relações, funções e constantes de B.

*Notação.* $(\mathrm{A}, S_1, \ldots, S_n, g_1, \ldots, g_m, \{a_j \mid j \in J\})$ é a expansão de A com os extras indicados.

No início (antes que "teoria dos modelos" foi introduzida) Skolem (1920) e Löwenheim (1915) estudaram as possíveis cardinalidades de modelos de teorias consistentes. A seguinte generalização segue imediatamente dos resultados precedentes.

**Teorema 3.2.3 (Teorema de Skolem–Löwenheim de-cima-para-baixo)** *Seja $\Gamma$ um conjunto de sentenças em uma linguagem de cardinalidade $\kappa$, e suponha que $\kappa < \lambda$. Se $\Gamma$ tem um modelo de cardinalidade $\kappa'$, com $\kappa \leq \kappa' < \lambda$.*

*Demonstração.* Adicione à linguagem $L$ de $\Gamma$ um conjunto de constantes novas (que não ocorrem no alfabeto de $L$) $\{c_i \mid i \in I\}$ de cardinalidade $\kappa'$, e considere $\Gamma' = \Gamma \cup \{c_i \neq c_j \mid i, j \in I, i \neq j\}$. Alegação: $\mathrm{Mod}(\Gamma) \neq \emptyset$.

Considere um modelo A de $\Gamma$ de cardinalidade $\lambda$. Expandimos A para $\mathrm{A}'$ adicionando $\kappa'$ constantes distintas (isso é possível: $|\mathrm{A}|$ contém um subconjunto de cardinalidade $\kappa'$. $\mathrm{A}' \in \mathrm{Mod}(T)$ (cf. Exercício 3) e $\mathrm{A}' \models c_i \neq c_j$ $(i \neq j)$. Consequentemente $\mathrm{Mod}(\Gamma) \neq \emptyset$. A cardinalidade da linguagem de $\Gamma'$ é $\kappa'$. Pelo Lema da Existência de Modelo $\Gamma'$ tem um modelo $\mathrm{B}'$ de cardinalidade $\leq \kappa'$, mas, pelos axiomas $c_i \neq c_j$, a cardinalidade é também $\geq \kappa'$. Logo $\mathrm{B}'$ tem cardinalidade $\kappa'$. Agora tome o reduto B de $\mathrm{B}'$ na linguagem de $\Gamma$, então $\mathrm{B} \in \mathrm{Mod}(\Gamma))$ (Exercício 3). $\square$

*Exemplos*

1. A teoria dos números reais, $\mathrm{Th}(R)$, na linguagem dos corpos, tem um modelo contável.

2. Considere a teoria de conjuntos de Zermelo–Fraenkel $ZF$. Se $\mathrm{Mod}(ZF) \neq \emptyset$, então $ZF$ tem um modelo contável. Esse fato foi descoberto por Skolem. Devido à sua natureza intrigante, ele foi chamado de *paradoxo de Skolem*. Pode-se provar em $ZF$ a existência de conjuntos incontáveis (e.g. o contínuo), como então pode $ZF$ ter um modelo contável? A resposta é simples: enumerabilidade vista de fora e de dentro do modelo não é o mesmo. Para estabelecer enumerabilidade precisa-se de uma bijeção com os números naturais. Aparentemente um modelo pode ser tão pobre que lhe falta bijeções que de fato existem fora do modelo.

**Teorema 3.2.4 (Teorema de Skolem–Löwenheim de-baixo-para-cima)** *Suponha que $\Gamma$ tenha uma linguagem de cardinalidade $\kappa$, e que $\mathrm{A} \in \mathrm{Mod}(\Gamma)$ com cardinalidade $\lambda \geq \kappa$. Para cada $\mu > \lambda$ $\Gamma$ tem um modelo de cardinalidade $\mu$.*

*Demonstração.* Adicione $\mu$ novas constantes $c_i$, $i \in I$ a $L$ e considere $\Gamma' = \Gamma \cup \{c_i \neq c_j \mid i \neq j, i, j \in I\}$. Alegação: $\mathrm{Mod}(\Gamma') \neq \emptyset$. Aplicamos o Teorema da Compaccidade.

Seja $\Delta \subseteq \Gamma'$ um conjunto finito. Digamos que $\Delta$ contém novos axiomas com constantes $c_{i_0}, \ldots, c_{i_k}$, então $\Delta \subseteq \Gamma \cup \{c_{i_p} \neq c_{i_q} \mid p, q \leq k\} = \Gamma_0$. Claramente cada modelo de $\Gamma_0$ é um modelo de $\Delta$ (Exercício 1(i)).

Agora tome A e expanda esse modelo para $\mathrm{A}' = (\mathrm{A}, a_1, \ldots, a_k)$, onde os $a_i$'s são distintos.

Então obviamente $\mathrm{A}' \in \mathrm{Mod}(\Gamma_0)$, logo $\mathrm{A}' \in \mathrm{Mod}(\Delta)$. Pelo Teorema da Compaccidade existe um $\mathrm{B}' \in \mathrm{Mod}(\Gamma')$. O reduto B de $\mathrm{B}'$ à (tipo da) linguagem $L$ é um modelo de $\Gamma$. Dos axiomas adicionais em $\Gamma'$ segue que $\mathrm{B}'$, e consequentemente B, tem cardinalidade $\geq \mu$.

Agora aplicamos o Teorema de Skolem–Löwenheim de-cima-para-baixo e obtemos a existência de um modelo de $\Gamma$ de cardinalidade $\mu$. $\square$

**Aplicação I. Modelos Não-padrão de PA.**

**Corolário 3.2.5** *A aritmética de Peano tem modelos não-padrão.*

Seja $\mathcal{P}$ a classe de todas as estruturas de Peano. Faça $\mathbf{PA} = \mathrm{Th}(\mathcal{P})$. Pelo Teorema da Completude $\mathbf{PA} = \{\sigma \mid \Sigma \vdash \sigma\}$ onde $\Sigma$ é o conjunto de axiomas listado na seção 2.7, Exemplo 6. **PA** tem um modelo de cardinalidade $\aleph_0$ (o modelo padrão N), logo pelo Teorema de Skolem–Löwenheim de-baixo-para-cima a teoria **PA** tem modelos de toda cardinalidade $k > \aleph_0$. Esses modelos são claramente não isomorfos a N. Para mais detalhes veja a Aplicação I da seção 3.3.

**Aplicação II. Modelos Finitos e Infinitos**

**Lema 3.2.6** *Se $\Gamma$ tem modelos finitos arbitrariamente grandes, então $\Gamma$ tem um modelo infinito.*

*Demonstração.* Faça $\Gamma' = \Gamma \cup \{\lambda_n \mid n > 1\}$, onde $\lambda_n$ expressa a sentença "existem pelo menos $n$ elementos distintos", cf. seção 2.7, Exemplo 1. Aplique o Teorema da Compaccidade. Seja $\Delta \subseteq \Gamma'$ finito, e seja $\lambda_m$ a sentença $\lambda_n$ em $\Delta$ com o maior índice $n$. Verifique que $\mathrm{Mod}(\Delta) \subseteq \mathrm{Mod}(T \cup \{\lambda_m\})$. Agora $\Gamma$ tem modelos finitos arbitrariamente grandes, logo $\Gamma$ tem um modelo A com no mínimo $m$ elementos, i.e. $\mathrm{A} \in \mathrm{Mod}(\Gamma \cup \{\lambda_m\})$. Logo $\mathrm{Mod}(\Delta) \neq \emptyset$.

Pela compaccidade $\mathrm{Mod}(\Gamma') \neq \emptyset$, mas em virtude dos axiomas $\lambda_m$, um modelo de $\Gamma'$ é infinito. Daí $\Gamma'$, e por conseguinte $\Gamma$, tem um modelo infinito. □

**Corolário 3.2.7** *Considere uma classe $\mathcal{K}$ de estruturas que tem modelos finitos arbitrariamente grandes. Então, na linguagem da classe, não existe conjunto $\Sigma$ de sentenças, tal que $\mathrm{A} \in \mathrm{Mod}(\Sigma) \Leftrightarrow \mathrm{A}$ é finito e $\mathrm{A} \in \mathcal{K}$.*

*Demonstração.* Imediata. □

Podemos parafrasear o resultado da seguinte forma: a classe de estruturas finitas em tal classe $\mathcal{K}$ não é axiomatizável em lógica de primeira ordem.

Todos nós sabemos que finitude pode ser expressa em uma linguagem que cont'em variáveis para conjuntos ou funções (e.g. a definição de Dedekind), portanto a incapacidade de caracterizar a noção de finito é um defeito específico da lógica de primeira ordem. Dizemos que *finitude não é uma propriedade de primeira ordem.*

O corolário se aplica a várias classes, e.g. grupos, anéis, corpos, conjuntos parcialmente ordenados, conjuntos (estruturas de identidade).

**Aplicação III. Axiomatizabilidade e Axiomatizabilidade Finita.**

**Definição 3.2.8** Uma classe $\mathcal{K}$ de estruturas é (finitamente) *axiomatizável* se existe um conjunto (finito) $\Gamma$ tal que $\mathcal{K} = \mathrm{Mod}(\Gamma)$. Dizemos que $\Gamma$ *axiomatiza* $\mathcal{K}$; as sentenças de $\Gamma$ são chamadas de axiomas (cf. 3.1.4) de $\mathcal{K}$.

Exemplos de conjuntos de axiomas $\Gamma$ para as classes de conjuntos parcialmente ordenados, conjuntos ordenados, grupos, anéis, estruturas de Peano, são listados na seção 2.7.

O seguinte fato é muito útil.

**Lema 3.2.9** *Se $\mathcal{K} = \mathrm{Mod}(\Gamma)$ e $\mathcal{K}$ é finitamente axiomatizável, então $\mathcal{K}$ é axiomatizável por um subconjunto finito de $\Gamma$.*

*Demonstração.* Seja $\mathcal{K} = \mathrm{Mod}(\Delta)$ para um $\Delta$ finito, então $\mathcal{K} = \mathrm{Mod}(\sigma)$, onde $\sigma$ é a conjunção de todas as sentenças de $\Delta$ (Exercício 4). Então $\sigma \models \psi$ para toda $\psi \in \Gamma$ e $\Gamma \models \sigma$, daí $\Gamma \vdash \sigma$ também. Por conseguinte existe um número finito $\psi_1, \ldots, \psi_k \in \Gamma$ tal que $\psi_1, \ldots, \psi_k \vdash \sigma$. Alegação: $\mathcal{K} = \mathrm{Mod}(\psi_1, \ldots, \psi_k)$.

(i) $\{\psi_1, \ldots, \psi_k\} \subseteq \Gamma$ logo $\mathrm{Mod}(\Gamma) \subseteq \mathrm{Mod}(\psi_1, \ldots, \psi_k)$.

(ii) De $\psi_1, \ldots, \psi_k \vdash \sigma$ segue que $\mathrm{Mod}(\psi_1, \ldots, \psi_k) \subseteq \mathrm{Mod}(\sigma)$.

Usando (i) e (ii) concluimos que $\mathrm{Mod}(\psi_1, \ldots, \psi_k) = \mathcal{K}$. □

Esse lema é instrumental para se demonstrar resultados de não-axiomatizabilidade-finita. Precisamos de mais um fato.

**Lema 3.2.10** *$\mathcal{K}$ é finitamente axiomatizável $\Leftrightarrow$ $\mathcal{K}$ e seu complemento $\mathcal{K}^c$ são ambas axiomatizáveis.*

*Demonstração.* $\Rightarrow$. Seja $\mathcal{K} = \mathrm{Mod}(\varphi_1, \ldots, \varphi_n)$, então $\mathcal{K} = \mathrm{Mod}(\varphi_1 \wedge \ldots \wedge \varphi_n)$. $\mathrm{A} \in \mathcal{K}^c$ (complemento de $\mathcal{K}$) $\Leftrightarrow$ $\mathrm{A} \not\models \varphi_1 \wedge \ldots \wedge \varphi_n \Leftrightarrow \mathrm{A} \models \neg(\varphi_1 \wedge \ldots \wedge \varphi_n)$. Logo $\mathcal{K}^c = \mathrm{Mod}(\neg(\varphi_1 \wedge \ldots \wedge \varphi_n))$.
$\Leftarrow$. Seja $\mathcal{K} = \mathrm{Mod}(\Gamma)$, $\mathcal{K}^c = \mathrm{Mod}(\Delta)$. $\mathcal{K} \cap \mathcal{K}^c = \mathrm{Mod}(\Gamma \cup \Delta) = \emptyset$ (Exercício 1). Pela compaccidade, existem $\varphi_1, \ldots, \varphi_n \in \Gamma$ e $\psi_1, \ldots, \psi_m \in \Delta$ tal que $\mathrm{Mod}(\varphi_1, \ldots, \varphi_n, \psi_1, \ldots, \psi_m) = \emptyset$, ou

$\mathrm{Mod}(\varphi_1, \ldots, \varphi_n) \cap \mathrm{Mod}(\psi_1, \ldots, \psi_m) = \emptyset$, (1)
$\mathcal{K} = \mathrm{Mod}(\Gamma) \subseteq \mathrm{Mod}(\varphi_1, \ldots, \varphi_n)$, (2)
$\mathcal{K}^c = \mathrm{Mod}(\Delta) \subseteq \mathrm{Mod}(\psi_1, \ldots, \psi_m)$, (3)

(1), (2), (3) $\Rightarrow \mathcal{K} = \mathrm{Mod}(\varphi_1, \ldots, \varphi_n)$. □

Agora obtemos uma série de corolários.

**Corolário 3.2.11** *A classe de todos os conjuntos infinitos (estruturas de identidade) é axiomatizável, porém não é finitamente axiomatizável.*

*Demonstração.* A é infinita $\Leftrightarrow$ $\mathrm{A} \in \mathrm{Mod}(\{\lambda_n \mid n \in \mathbb{N}\})$. Logo o conjunto de axiomas é $\{\lambda_n \mid n \in \mathbb{N}\}$. Por outro lado a classe de conjuntos finitos não é axiomatizável, logo, pelo Lema 3.2.10, a classe de conjuntos infinitos não é finitamente axiomatizável. □

**Corolário 3.2.12** (i) *A classe dos corpos de característica* $p$ $(> 0)$ *é finitamente axiomatizável.*

(ii) *A classe dos corpos de característica* 0 *é axiomatizável mas não é finitamente axiomatizável.*

(iii) *A classe dos corpos de característica positiva não é axiomatizável.*

*Demonstração.* (i) A teoria dos corpos tem um conjunto finito de axiomas $\Delta$. $\Delta \cup \{\overline{p} = 0\}$ axiomatiza a classe $\mathcal{F}_p$ de corpos de característica $p$ (onde $\overline{p}$ significa $1 + \ldots + 1$, $p$ vezes).

(ii) $\Delta \cup \{\overline{2} \neq 0, \overline{3} \neq 0, \ldots, \overline{p} \neq 0, \ldots\}$ axiomatiza a classe $\mathcal{F}_0$ de corpos de característica 0. Suponha que $\mathcal{F}_0$ fosse finitamente axiomatizável, então pelo Lema 3.2.9 $\mathcal{F}_0$ era axiomatizável por $\Gamma = \Delta \cup \{\overline{p}_1 \neq 0, \ldots, \overline{p}_k \neq 0\}$, onde $p_1, \ldots, p_k$ são primos (não necessariamente os primeiros $k$ primos). Seja $q$ um número primo maior que todos os $p_i$'s (Euclides). Então $\mathbb{Z}/(q)$ (os inteiros módulo $q$) é um modelo de $\Gamma$, mas $\mathbb{Z}/(q)$ não é um corpo de característica 0. Contradição.

(iii) Observe que se $\Gamma$ axiomatiza os corpos de característica positiva, então $\Gamma \cup \{\overline{2} \neq 0, \overline{3} \neq 0, \ldots, \overline{p} \neq 0, \ldots\}$ é consistente. □

**Corolário 3.2.13** *A classe* $A_c$ *de todos os corpos algebricamente fechados é axiomatizável mas não é finitamente axiomatizável.*

*Demonstração.* Seja $\sigma_n = \forall y_1 \ldots y_n \exists x(x^n + y_1 x^{n-1} + \ldots + y_{n-1}x + y_n = 0)$. Então $\Gamma = \Delta \cup \{\sigma_n \mid n \geq 1\}$ ($\Delta$ tal qual no corolário 3.2.12) axiomatiza $A_c$. Para mostrar não-axiomatizabilidade-finita, aplique o Lema 3.2.9 a $\Gamma$ e encontre um corpo no qual um certo polinômio não fatora. □

**Corolário 3.2.14** *A classe de todos os grupos abelianos livres-de-torsão é axiomatizável mas não é finitamente axiomatizável.*

*Demonstração.* Exercício 14. □

*Observação.* No Lema 3.2.9 usamos o Teorema da Completude e no Lema 3.2.10 o Teorema da Compaccidade. A vantagem de usar apenas o Teorema da Compaccidade é que se evita totalmente a noção de demonstrabilidade. O leitor poderia objetar que essa vantagem é um tanto artificial pois o Teorema da Compaccidade é um corolário do Teorema da Completude. Isso é verdade na nossa apresentação; pode-se, no entanto, derivar o Teorema da Compaccidade através de meios puramente da teoria dos modelos (usando ultraprodutos, cf. Chang–Keisler), portanto existem situações em que se tem que usar o Teorema da Compaccidade. No momento a escolha entre usar o Teorema da Completude ou o Teorema da Compaccidade é em grande medida uma questão de gosto ou conveniência.

Para efeito de ilustração faremos uma demonstração alternativa do Lema 3.2.9 usando o Teorema da Compaccidade:

Novamente temos que $\mathrm{Mod}(\Gamma) = \mathrm{Mod}(\sigma)$ $(*)$. Considere $\Gamma' = \Gamma \cup \{\neg\sigma\}$.

$$\begin{aligned} \mathfrak{A} \in \mathrm{Mod}(\Gamma') \quad &\Leftrightarrow \mathfrak{A} \in \mathrm{Mod}(\Gamma) \quad \text{e} \quad \mathfrak{A} \models \neg\sigma, \\ &\Leftrightarrow \mathfrak{A} \in \mathrm{Mod}(\Gamma) \quad \text{e} \quad \mathfrak{A} \notin \mathrm{Mod}(\sigma). \end{aligned}$$

Em vista de $(*)$ temos que $\mathrm{Mod}(\Gamma') = \emptyset$.

Pelo Teorema da Compaccidade existe um subconjunto finito $\Delta$ de $\Gamma'$ com $\mathrm{Mod}(\Delta) = \emptyset$. Nada impede que se suponha que $\neg\sigma \in \Delta$, daí $\mathrm{Mod}(\psi_1, \ldots, \psi_k, \neg\sigma) = \emptyset$. Agora segue facilmente que $\mathrm{Mod}(\psi_1, \ldots, \psi_k) = \mathrm{Mod}(\sigma) = \mathrm{Mod}(\Gamma)$. $\square$

**Aplicação IV. Ordenando Conjuntos.**

Demonstra-se facilmente que cada conjunto finito pode ser ordenado, enquanto que para conjuntos infinitos isso é mais difícil. Um truque simples é apresentado abaixo.

**Teorema 3.2.15** *Cada conjunto infinito pode ser ordenado.*

*Demonstração.* Seja $|X| = \kappa \geq \aleph_0$. Considere $\Gamma$, o conjunto de axiomas para ordens lineares (2.7.3). $\Gamma$ tem um modelo contável, e.g. $\mathbb{N}$. Pelo Teorema de Skolem–Löwenheim de-baixo-para-cima $\Gamma$ tem um modelo $\mathfrak{A} = \langle A, < \rangle$ de cardinalidade $\kappa$. Como $X$ e $Z$ têm a mesma cardinalidade existe uma bijeção $f : X \to A$. Defina $x < x' := f(x) < f(x')$. Evidentemente, $<$ é uma ordem linear.

Da mesma maneira obtém-se: Cada conjunto infinito pode ser densamente ordenado. O mesmo truque funciona para classes axiomatizáveis em geral.

**Exercícios**

1.

Mostre que:
(i) $\Gamma \subseteq \Delta \Rightarrow \mathrm{Mod}(\Delta) \subseteq \mathrm{Mod}(\Gamma)$,
(ii) $\mathcal{K}_1 \subseteq \mathcal{K}_2 \Rightarrow \mathrm{Th}(\mathcal{K}_2) \subseteq \mathrm{Th}(\mathcal{K}_1)$,
(iii) $\mathrm{Mod}(\Gamma \cup \Delta) = \mathrm{Mod}(\Gamma) \cap \mathrm{Mod}(\Delta)$,
(iv) $\mathrm{Th}(\mathcal{K}_1 \cup \mathcal{K}_2) = \mathrm{Th}(\mathcal{K}_1) \cap \mathrm{Th}(\mathcal{K}_2)$,
(v) $\mathcal{K} \subseteq \mathrm{Mod}(\Gamma) \Leftrightarrow \Gamma \subseteq \mathrm{Th}(\mathcal{K})$,
(vi) $\mathrm{Mod}(\Gamma \cap \Delta) \supseteq \mathrm{Mod}(\Gamma) \cup \mathrm{Mod}(\Delta)$,
(vii) $\mathrm{Th}(\mathcal{K}_1 \cap \mathcal{K}_2) \supseteq \mathrm{Th}(\mathcal{K}_1) \cup \mathrm{Th}(\mathcal{K}_2)$.

Mostre que em (vi) e (vii) $\supseteq$ não pode ser substituído por $=$.

2. (i) $\Gamma \subseteq \mathrm{Th}(\mathrm{Mod}(\Gamma))$,
   (ii) $\mathcal{K} \subseteq \mathrm{Mod}(\mathrm{Th}(\mathcal{K}))$,
   (iii) $\mathrm{Th}(\mathrm{Mod}(\Gamma))$ é uma teoria com $\Gamma$ como conjunto de axiomas.

3. Se $\mathfrak{A}$ com linguagem $L$ é um reduto de $\mathfrak{B}$, então $\mathfrak{A} \models \sigma \Leftrightarrow \mathfrak{B} \models \sigma$ para $\sigma \in L$.

4. $\mathrm{Mod}(\varphi_1, \ldots, \varphi_n) = \mathrm{Mod}(\varphi_1 \wedge \ldots \wedge \varphi_n)$.

5. $\Gamma \models \varphi \Rightarrow \Delta \models \varphi$ para um subconjunto finito $\Delta \subseteq \Gamma$. (Dê uma prova usando a completude, e uma outra prova usando a compaccidade sobre $\Gamma \cup \{\neg\varphi\}$).

6. Mostre que *boa-ordenação* não é uma noção de primeira ordem. Suponha que $\Gamma$ axiomatiza a classe de boas-ordenações. Adicione um número finito de constantes $c_i$ e mostre que $\Gamma \cup \{c_{i+1} < c_i \mid i \in \mathcal{N}\}$ tem um modelo.

7. Se $\Gamma$ tem apenas modelos finitos, então existe um $n$ tal que cada modelo tem pelo menos $n$ elementos.

8. Suponha que $L$ tenha o símbolo binário de predicado $P$. $\sigma := \forall x \neg P(x,x) \wedge \forall xyz(P(x,y) \wedge P(y,z) \rightarrow P(x,z)) \wedge \forall x \exists y P(x,y)$. Mostre que $\mathrm{Mod}(\sigma)$ contém apenas modelos infinitos.

9. Mostre que $\sigma \vee \forall xy(x = y)$ tem modelos infinitos e um modelo finito, mas nenhum modelo finito arbitrariamente grande ($\sigma$ tal qual no exercício anterior).

10. Suponha que $L$ tenha um símbolo unário de função.
    (i) Escreva uma sentença $\varphi$ tal que $\mathfrak{A} \models \varphi \Leftrightarrow f^{\mathfrak{A}}$ seja uma sobrejeção.
    (ii) Idem para uma injeção.
    (iii) Idem para uma bijeção (permutação).
    (iv) Use (ii) para formular uma sentença $\sigma$ tal que $\mathfrak{A} \models \varphi \Leftrightarrow \mathfrak{A}$ é infinito (Dedekind).
    (v) Mostre que cada conjunto infinito carrega uma permutação sem pontos fixos (cf. a demonstração de 3.2.15).

11. Mostre que: $\sigma$ se verifica para corpos de característica zero $\Rightarrow \sigma$ se verifica para todos os corpos de característica $q > p$ para um certo $p$.

12. Considere uma seqüência de teorias $T_i$ tal que $T_i \neq T_{i+1}$ e $T_i \subseteq T_{i+1}$. Mostre que $\bigcup\{T_i \mid i \in \mathcal{N}\}$ não é finitamente axiomatizável.

13. Se $T_1$ e $T_2$ são teorias tais que $\mathrm{Mod}(T_1 \cup T_2) = \emptyset$, então existe uma $\sigma$ tal que $T_1 \models \sigma$ e $T \models \neg\sigma$.

14. Demonstre o Corolário 3.2.14.

15. Mostre que cada conjunto ordenado contável pode ser imerso nos racionais.

16. Mostre que a classe das árvores não pode ser axiomatizada. Aqui definimos uma árvore como uma estrutura $\langle T, \leq, t \rangle$, onde $\leq$ é uma ordem parcial, tal que para cada $a$ os predecessores formam uma cadeia finita $a = a_n < a_{n-1} < \ldots < a_1 < a_0 = t$. $t$ é chamado de elemento topo.

## 3.3 Algo de Teoria dos Modelos

Na teoria dos modelos se investiga as várias propriedades de modelos (estruturas), em particular em conexão com as características de suas linguagens. Poder-se-ia dizer que a álgebra é parte da teoria dos modelos, e algumas partes da álgebra de fato pertencem à teoria dos modelos, outras partes apenas no sentido do caso limite no qual o papel da linguagem é desprezível. É a interação entre linguagens e modelos que faz com que a teoria dos modelos seja fascinante. Aqui apenas discutiremos os preliminares do tópico.

Em álgebra não se distingue estruturas que são isomorfas; a natureza dos objetos é puramente acidental. Em lógica temos um outro critério: distinguimos entre duas estruturas exibindo uma sentença que se verifica numa mas não se verifica na outra. Portanto, se $\mathrm{A} \models \sigma \Leftrightarrow \mathrm{B} \models \sigma$ para toda $\sigma$, então não podemos distinguir (logicamente) A e B.

**Definição 3.3.1** (i) $f : |\mathrm{A}| \to |\mathrm{B}$ é um *homomorfismo* se $\langle a_1, \ldots, a_k \rangle \in P_i^{\mathrm{A}} \Rightarrow \langle f(a_1), \ldots, f(a_k) \rangle \in P_i^{\mathrm{B}}$ para todo $P_i$, $f(F_j^{\mathrm{A}}(a_1, \ldots, a_p)) = F_j^{\mathrm{B}}(f(a_1), \ldots, f(a_p))$ para todo $F_j$, e $f(c^{\mathrm{A}}) = c_i^{\mathrm{B}}$, para todo $c_i$.

(ii) $f$ é um *isomorfismo* se ela é um homomorfismo que é bijetor e satisfaz $\langle a_1, \ldots, a_n \rangle \in P_i^{\mathrm{A}} \Leftrightarrow \rangle f(a_1), \ldots, f(a_n) \rangle \in P_i^{\mathrm{B}}$, para todo $P_i$.

Escrevemos $f : \mathrm{A} \to \mathrm{B}$ se $f$ é um homomorfismo de A para B. $\mathrm{A} \cong \mathrm{B}$ significa "A é isomorfa a B, i.e. existe um isomorfismo $f : \mathrm{A} \to \mathrm{B}$.

**Definição 3.3.2** A e B são elementarmente equivalentes se para todas as sentenças $\sigma$ de $L$, $\mathrm{A} \models \sigma \Leftrightarrow \mathrm{B} \models \sigma$.

*Notação.* $\mathrm{A} \equiv \mathrm{B}$. Note que $\mathrm{A} \equiv \mathrm{B} \Leftrightarrow \mathrm{Th(A)} = \mathrm{Th(B)}$.

**Lema 3.3.3** $\mathrm{A} \cong \mathrm{B} \Rightarrow \mathrm{A} \equiv \mathrm{B}$.

*Demonstração.* Exercício 4. □

**Definição 3.3.4** A é uma *subestrutura* (submodelo) de B (do mesmo tipo) se $|\mathrm{A}| \subseteq |\mathrm{B}|$; $P_i^{\mathrm{B}} \cap |\mathrm{A}|^n = P_i^{\mathrm{A}}$, $F^{\mathrm{B}} \restriction |\mathrm{A}|^n = F_j^{\mathrm{A}}$ e $c_i^{\mathrm{A}} = c_i^{\mathrm{B}}$ (onde $n$ é o número de argumentos da função).

*Notação.* Note que não é suficiente que A esteja contida em B "enquanto conjuntos"; as relações e funções de B têm que ter extensões das relações e funções correspondentes em A, da maneira especificada acima.

*Exemplos.* O corpo dos racionais é uma subestrutura do corpo dos reais, mas não do corpo ordenado dos reais. Seja A o grupo aditivo dos racionais, B o grupo multiplicativo dos racionais não-nulos. Embora $|\mathrm{B}| \subseteq |\mathrm{A}|$, B não é uma subestrutura de A. As noções conhecidas de subgrupos, sub-anéis, subespaços, todas satisfazem a definição acima.

A noção de equivalência elementar apenas requer que sentenças (que não se referem a elementos específicos, exceto constantes) sejam simultaneamente verdadeiras em duas estruturas. Podemos refinar a noção, considerando $\mathrm{A} \subseteq \mathrm{B}$ e permitindo a referência a elementos de $|\mathrm{A}|$.

**Definição 3.3.5** A é uma *subestrutura elementar* de B (ou que B é uma *extensão elementar* de A) se $A \subseteq B$ e para toda $\varphi(x_1, \ldots, x_n)$ em $L$ e $a_1, \ldots, a_n \in |A|$, $A \models \varphi(\overline{a}_1, \ldots, \overline{a}_n) \Leftrightarrow B \models \varphi(\overline{a}_1, \ldots, \overline{a}_n)$.

*Notação.* $A \prec B$.

Dizemos que A e B têm as mesmas sentenças verdadeiras *com parâmetros in* A.

**Fato 3.3.6** $A \prec B \Rightarrow A \equiv B$.

A recíproca não se verifica (cf. Exercício 6).

Como frequentemente usaremos todos os elementos de $|A|$ a A como constantes, é conveniente se ter uma notação especial para a estrutura enriquecida: $\hat{A} = (A, |A|)$.

Se se deseja descrever uma certa estrutura A, é preciso especificar todas os relacionamentos básicos e relações funcionais. Isso pode ser feito na linguagem $L(A)$ associada a A (que, incidentalmente, *é* a linguagem do tipo de $\hat{A}$).

**Definição 3.3.7** *O diagrama*, Diag(A), é o conjunto de átomos fechados e negações de átomos fechados de $L(A)$, que são verdadeiros em A. O *diagrama positivo*, $\mathrm{Diag}^+(A)$, é o conjunto de átomos fechados $\varphi$ de $L(A)$ tais que $A \models \varphi$.

*Exemplo.*

1. $A = \langle \mathbb{N} \rangle$. $\mathrm{Diag}(A) = \{\overline{n} = \overline{n} \mid n \in \mathbb{N}\} \cup \{\overline{n} \neq \overline{m} \mid n, m \in \mathbb{N}\}$.
2. $B = \langle \{1, 2, 3\}, < \rangle$. (ordem natural). $\mathrm{DiagB}) = \{\overline{1} = \overline{1}, \overline{2} = \overline{2}, \overline{3} = \overline{3}, \overline{1} \neq \overline{2}, \overline{2} \neq \overline{3}, \overline{2} \neq \overline{1}, \overline{3} \neq \overline{1}, \overline{3} \neq \overline{2}, \overline{1} < \overline{2}, \overline{1} < \overline{3}, \overline{2} < \overline{3}, \neg\overline{2} < \overline{1}, \neq \overline{3} < \overline{2}, \neg\overline{3} < \overline{1}, \neg\overline{1} < \overline{1}, \neg\overline{2} < \overline{2}, \neg\overline{3} < \overline{3}\}$.

Diagramas são úteis para muitos propósitos. Demonstramos um deles aqui: Dizemos que A é *isomorficamente imerso* em B se existe um isomorfismo $f$ de A em uma subestrutura de B.

**Lema 3.3.8** *A é isomorficamente imersa em* $B \Leftrightarrow \hat{B}$ *é um modelo de* Diag(A).

*Demonstração.* $\Rightarrow$. Seja $f$ uma imersão isomórfica de A em B, então $A \models P_1(\overline{a}_1, \ldots, \overline{a}_n) \Leftrightarrow B \models P_1(\overline{f(a_1)}, \ldots, \overline{f(a_n)})$ e $A \models t(\overline{a}_1, \ldots, \overline{a}_n) = s(\overline{a}_1, \ldots, \overline{a}_n) \Leftrightarrow B \models t(\overline{f(a_1)}, \ldots) = s(\overline{f(a_1)}, \ldots)$ (cf. Exercício 4.). Interpretando $\overline{a}$ como $f(a)$ em $\hat{B}$ (i.e. $\overline{a}^B = f(a)$), vemos imediatamente que $\hat{B} \models \mathrm{Diag}(A)$.
$\Leftarrow$. Seja $\hat{B} \models \mathrm{Diag}(A)$. Defina uma função $f : |A| \to |B|$ da seguinte maneira: $f(a) = (\overline{a})^B$. Então, claramente, $f$ satisfaz as condições da definição 3.3.1 sobre relações e funções (pois elas são dadas por átomos e negações de átomos). Além do mais se $a_1 \neq a_2$ então $A \models \neg\overline{a}_1 = \overline{a}_2$, logo $\hat{B} \models \neg\overline{a}_1 = \overline{a}_2$.

Daí $\overline{a}_1^B \neq \overline{a}_2^B$, e portanto $f(a_1) \neq f(a_2)$. Isso mostra que $f$ é um isomorfismo. $\square$

Frequentemente identificaremos A com sua imagem sob uma imersão isomórfica em B, de modo que possamos considerar A como uma subestrutura de B.

Temos um critério semelhante para extensão elementar. Dizemos que A é *elementarmente imersível* em B se $A \cong A'$ e $A' \prec B$ para alguma estrutura $A'$. Novamente, simplificaremos frequentemente as coisas escrevendo simplesmente $A \prec B$ quando queremos dizer "elementarmente imersível".

**Lema 3.3.9** $\mathrm{A} \prec \mathrm{B} \Leftrightarrow \hat{\mathrm{B}} \models \mathrm{Th}(\hat{\mathrm{A}})$.

Note bem: $\mathrm{A} \prec \mathrm{B}$ se verifica "a menos de isomorfismo". Supõe-se que $\hat{\mathrm{B}}$ é de um tipo de similaridade que admite no mínimo constantes para todos os símbolos de constante de $L(\mathrm{A})$.

*Demonstração.* $\Rightarrow$. Seja $\varphi(\overline{a}_1, \ldots, \overline{a}_n) \in \mathrm{Th}(\hat{\mathrm{A}})$, então $\mathrm{A} \models \varphi(\overline{a}_1, \ldots, \overline{a}_n)$, donde $\hat{\mathrm{B}} \models \varphi(\overline{a}_1, \ldots, \overline{a}_n)$. Logo $\hat{\mathrm{B}} \models \mathrm{Th}(\hat{\mathrm{A}})$.

$\Leftarrow$. Por 3.3.8, $\mathrm{A} \subseteq \mathrm{B}$ (a menos de isomorfismo). Agora o leitor pode facilmente concluir a demonstração. □

Agora vamos dar algumas aplicações.

**Aplicação I. Modelos Não-padrão da Aritmética.**

Recordemos que $\mathrm{N} = \langle \mathbb{N}, +, \cdot, s, 0 \rangle$ é o *modelo padrão* da aritmética. Sabemos que ele satisfaz os axiomas de Peano (cf. exemplo 6, seção 2.7). Usamos as abreviações introduzidas na seção 2.7.

Vamos agora construir um modelo não-padrão. Considere $T = \mathrm{Th}(\hat{\mathrm{N}})$. Pelo Teorema de Skolem–Löwenheim $T$ tem um modelo incontável M. Como $\mathrm{M} \models \mathrm{Th}(\hat{\mathrm{N}})$, temos que, por 3.3.9, $\mathrm{N} \prec \mathrm{M}$. Observe que $\mathrm{N} \not\cong \mathrm{M}$ (por que?). Olharemos mais de perto para a forma pela qual N é imersa em M.

Notamos que
$$
\begin{array}{lll}
\mathrm{N} \models & \forall xyz(x < y \wedge y < z \rightarrow x < z) & (1) \\
\mathrm{N} \models & \forall xyz(x < y \vee x = y \vee y < x) & (2) \\
\mathrm{N} \models & \forall x(\overline{0} \leq x) & (3) \\
\mathrm{N} \models & \neg \exists x(\overline{n} < x \wedge x < \overline{n+1}) & (4)
\end{array}
$$

Daí, N sendo uma subestrutura elementar de M, temos (1) e (2) para M, i.e. M é linearmente ordenado. De $\mathrm{N} \prec \mathrm{M}$ e (3) concluimos que $\overline{0}$ é o primeiro elemento de M. Além disso, (4) com $\mathrm{N} \prec \mathrm{M}$ nos diz que não existem elementos de M entre os "números naturais padrão".

Como resultado vemos que N é um segmento inicial de M

figura pagina 123

Observação: é importante se dar conta de que (1)–(4) não são apenas *verdadeiras no modelo padrão*, mas são até mesmo demonstráveis em **PA**. Isso implica que elas se verificam não apenas em extensões elementares de N, mas em *todas* as estruturas de Peano. O preço que se tem que pagar é a demonstração propriamente dita de (1)–(4) em **PA**, que é mais trabalhosa que simplesmente estabelecer sua validade em N. Entretanto, qualquer um que possa dar uma demonstração informal dessas propriedades simples descobrirão que é apenas um passo a mais (enfandonho, porém não difícil) para formalizar a prova em nosso sistema de dedução. Provas passo-a-passo são delineadas nos Exercícios 29, 30.

Portanto, todos os elementos de $|\mathrm{M}| - |\mathrm{N}|$, os *números não-padrão*, vêm após os números padrão. Como M é incontável, existe pelo menos um número não-padrão $a$. Note que $n < a$ para todo $n$, logo M tem uma *ordem não-arquimedeana* (recordemos que $n = 1 + 1 + \ldots + 1$ ($n$ vezes)).

Vemos que o sucessor $S(n) = n+1$ de um número padrão é padrão. Além do mais, $\mathrm{N} \models \forall x(x \neq \overline{0} \rightarrow \exists y(y + \overline{1} = x))$, portanto, como $\mathrm{N} \prec \mathrm{N}$, temos também que $\mathrm{M} \models \forall x(x \neq \overline{0} \rightarrow \exists x(y + \overline{1}))$, i.e. em M cada número, distinto de zero, tem um predecessor (único). Como $a$ é não-padrão ele é distinto de zero, daí ele tem um predecessor, digamos $a_1$. Como sucessores de números padrão são padrão, $a_1$ é não-padrão. Podemos repetir esse procedimento indefinidamente e obter uma seqüência descendente infinita $a > a_1 > a_2 > a_3 > \ldots$ de números não-padrão. Conclusão: a estrutura M não é bem-fundada.

Entretanto, subconjuntos *definíveis* não-vazios de M de fato possuem um elemento mínimo. Pois, tal conjunto é da forma $\{b \mid \mathrm{M} \models \varphi(\overline{b})\}$, onde $\varphi \in L(\mathrm{M})$, e sabemos que $\mathrm{N} \models \exists x \varphi(x) \to \exists x(\varphi(x) \wedge \forall y(\varphi(y) \to x \leq y))$. Essa sentença também se verifica em M e nos diz que $\{b \mid \mathrm{M} \models \varphi(\overline{b})\}$ tem um elemento mínimo se não for vazio.

A construção acima não apenas deu uma estrutura de Peano não-padrão (cf. 3.2.5), mas também um modelo não-padrão da *verdadeira aritmética*, i.e. é um modelo de todas as sentenças verdadeiras no modelo padrão. Além do mais, esse modelo não-padrão é uma extensão elementar.

Os modelos não-padrão de **PA** que são extensões elementares de N são aqueles que podem ser manuseados mais facilmente que os outros, pois os fatos do modelo padrão se transferem. Existem também um bom número de propriedades que têm sido estabelecidas para modelos não-padrão em geral. Tratamos duas delas aqui:

**Teorema 3.3.10** *O conjunto de números padrão em um modelo não-padrão não é definível.*

*Demonstração*. Suponha que exista uma $\varphi(x)$ na linguagem de **PA**, tal que: $\mathrm{M} \models \varphi(\overline{a}) \Leftrightarrow$ "$a$ é um número padrão", então $\neg\varphi(x)$ define os números não-padrão. Como **PA** prova o *princípio do menor número*, temos que $\mathrm{M} \models \exists x(\neg\varphi(x) \wedge \forall y < x\, \varphi(y))$, ou existe um menor número não-padrão. Entretanto, como vimos acima, isso não é o caso. Logo não existe tal definição. □

Uma conseqüência simples é o

**Lema 3.3.11 (Lema do Transbordamento)** *Se $\varphi(\overline{n})$ se verifica em um modelo não-padrão para uma quantidade infinita de números $n$, então $\varphi(a)$ se verifica para no mínimo um número infinito $a$.*

*Demonstração*. Suponha que para nenhum $a$ infinito $\varphi(\overline{a})$ se verifique, então $\exists y(x < \wedge\varphi(y))$ define o conjunto dos números naturais padrão no modelo. Isso contradiz o resultado precedente. □

Nossa técnica de construir modelos produz vários modelos não-padrão da aritmética de Peano. Não temos nesse estágio qualquer meio de decidir se todos os modelos de **PA** são elementarmente equivalentes ou não. A resposta a essa questão é fornecida pelo teorema da incompletude de Gödel, que enuncia que existe uma sentença $\gamma$ tal que **PA** $\nvdash \gamma$ e **PA** $\nvdash \neg\gamma$. A incompletude de **PA** tem sido re-estabelecida por meios bem diferentes por Paris–Kirby–Harrington, Kripke, e outros. Como resultado, temos agora exemplos para $\gamma$, que pertence à 'matemática normal', enquanto que a $\gamma$ de Gödel, embora puramente aritmética, pode ser considerada como um pouco artificial, cf. Barwise, *Handbook of Mathematical Logic*, D8. **PA** tem um modelo decidível (recursivo), a saber o modelo padrão. Esse, entretanto, é o único. Pelo teorema de Tennenbaum todos os modelos não-padrão de **PA** são indecidíveis (não recursivos).

**Aplicação II. Números Reais Não-padrão.**

Da mesma forma que na aplicação acima, podemos introduzir modelos não-padrão para o sistema de números reais. Usamos a linguagem do corpo ordenado $R$ de números reais, e por conveniência usamos o símbolo de função $||$, para a função do valor absoluto. Pelo Teorema de Skolem–Löwenheim existe um modelo $^*R$ de $\mathrm{Th}(\hat{R})$ tal que $^*R$ tem cardinalidade maior que a de $R$. Aplicando 3.3.9, vemos que $R \prec {}^*R$, portanto $^*R$ é um corpo ordenado, contendo os números reais padrão. Por razões de cardinalidade existe um elemento $a \in |{}^*R| - |R|$. Para o elemento $a$ existem duas possibilidades:

(i) $|a| > |r|$ para todo $r \in |R|$,

(ii) existe um $r \in |R|$ tal que $|a| < r$.

No segundo caso $\{u \in |R| \mid u < |a|\}$ é um subconjunto não-vazio limitado, que por conseguinte tem um supremo $s$ (em $R$). Como $|a|$ é um número não-padrão, não existe número padrão entre $s$ e $|a|$. Por álgebra, não existe número padrão entre 0 e $|\ |a| - s\ |$. Daí $|\ |a| -\ |^{-1}$ é maior que todos os números padrão. Elementos satisfazendo a condição (i) acima, são chamados *infinitos* e elementos satisfazendo (ii) são chamados *finitos* (note que os números padrão são finitos).

Agora vamos listar um número de fatos, deixando as demonstrações (bastante simples) ao leitor.

1. $^*R$ tem uma ordem não-arquimedeana.

2. Existem números $a$ tais que para todo número padrão positivo $r$, $0 < |a| < r$.

   Chamamos tais números, incluindo o 0, de *infinitesimais*.

3. $a$ é infinitesimal $\Leftrightarrow a^{-1}$ é infinito.

4. Para cada número não-padrão finito $a$ existe um único número padrão $pad(a)$ tal que $a - pad(a)$ é infinitesimal.

   Infinitesimais podem ser usados para cálculo elementar na tradição Leibniziana. Daremos alguns exemplos. Considere uma expansão $R'$ de $R$ com um predicado para $N$ e uma função $v$. Seja $^*R'$ o modelo não-padrão correspondente tal que $R' \prec {}^*R'$. Estamos na verdade considerando duas extensões ao mesmo tempo. $N$ é obtida em $R'$, i.e. distinguida por um predicado especial $N$. Daí $N$ é estendida, juntamente com $R'$ para $^*N$. Como é de se esperar $^*N$ é uma extensão elementar de $N$ (cf. Exercício 16). Por conseguinte, podemos ter confianą em operar da maneira tradicional com os números reais e os números naturais. Em particular temos em $^*R'$ números naturais infinitos disponíveis também. Queremos que $v$ seja uma seqüência, i.e. estamos apenas interessados nos valores de $v$ para argumentos sobre os números naturais. Os conceitos de convergência, limite, etc. podem ser trazidos de análise matemática.

   Usaremos a notação do cálculo. O leitor pode tentar dar a formulação correta.

   Aqui vai um exemplo: $\exists m \forall n > m(|v_n - v_m| < \epsilon)$ significa $\exists x(N(x) \wedge \forall y(N(y) \wedge y > x \to |v(y) - v(x)| < \epsilon)$. A rigor deveríamos relativizar os quantificadores sobre os números naturais (cf. 2.5.12), porém é mais conveniente usar variáveis de vários tipos.

5. A seqüência $v$ (ou $(v_n)$) converge em $R'$ sse para todos os números naturais $n, m$ $|v_n - v_m|$ é infinitesimal.

   *Demonstração.* $(v_n)$ converge em $R'$ se $R' \models \forall\epsilon > 0\exists n\forall m > n(|v_n - v_m| < \epsilon)$. Assuma que $(v_n)$ converge. Escolha para $\epsilon > 0$ um $n(\epsilon) \in |R'|$ tal que $R' \models \forall m > n(\epsilon)(|v_n - v_m| < \epsilon)$. Então temos também que ${}^*R' \models \forall m > n(\epsilon)(|v_n - v_m| < \epsilon)$. Em particular, se $m, m'$ são infinitos, então $m, m' > n(\epsilon)$ para todo $\epsilon$. Daí $|v_m - v_{m'}| < 2\epsilon$ para todo $\epsilon$. Isso significa que $|v_m - v_{m'}|$ é infinitesimal. Reciprocamente, se $|v_n - v_m|$ é infinitesimal para todos $n, m$ infinitos, então ${}^*R \models \forall m > n(|v_n - v_m| < \epsilon)$ onde $n$ é infinito e $\epsilon$ é padrão, positivo. Logo ${}^*R' \models \exists n\forall m > n(|v_n - v_m| < \epsilon)$, para cada número padrão $\epsilon > 0$. Agora, como $R' \prec {}^*R'$, temos $R' \models \exists n\forall m > n(|v_n - v_m| < \epsilon)$ para $\epsilon > 0$, logo $R' \models \forall\epsilon > 0\exists n\forall m > n(|v_n - v_m| < \epsilon)$. Daí $(v_n)$ converge. □

6. $\lim_{n\to\infty} v_n = a \Leftrightarrow |a - v_n|$ é infinitesimal para $n$ infinito.

   *Demonstração.* Semelhante à do item anterior. □

Fomos capazes de apenas tocar a superfície da chamada "análise não-padrão". Para um tratamento extensivo, veja e.g. *Robinson*, *Stroyan–Luxemburg*.

Podemos agora fortalecer os Teoremas de Skolem–Löwenheim.

**Teorema 3.3.12 (Skolem–Löwenheim de-cima-para-baixo)** *Suponha que a linguagem $L$ de* A *tenha cardinalidade $\kappa$, e suponha que* A *tenha cardinalidade $\lambda \geq \kappa$. Então existe uma estrutura* A *de cardinalidade $\kappa$ tal que* B $\prec$ A.

*Demonstração.* Veja corolário 3.4.11. □

**Teorema 3.3.13 (Skolem–Löwenheim de-baixo-para-cima)** *Suponha que a linguagem $L$ de* A *tenha cardinalidade $\kappa$ e que* A *tenha cardinalidade $\lambda \geq \kappa$. Então para cada $\mu > \lambda$ existe uma estrutura* B *de cardinalidade $\mu$, tal que* A $\prec$ B.

*Demonstração.* Aplique o velho Teorema de Skolem–Löwenheim de-baixo-para-cima à teoria Th($\hat{\mathrm{A}}$). □

Na prova de completude usamos teorias maximamente consistentes. Em teoria dos modelos essas teorias são chamadas de teorias completas. Via de regra, essa noção é definida com respeito a conjuntos de axiomas.

**Definição 3.3.14** Uma teoria com axiomas $\Gamma$ na linguagem $L$, é chamada *completa* se para cada sentença $\sigma$ em $L$, $\Gamma \vdash \sigma$ ou $\Gamma \vdash \neg\sigma$.

Uma teoria completa, por assim dizer, não deixa questões em aberto, mas ela não restringe a priori a classe de modelos. Antigamente os matemáticos tentavam encontrar teorias básicas desse tipo tais como axiomas para a aritmética que determinariam a menos de isomorfismo um modelo, i.e. tentavam dar um conjunto $\Gamma$ de axiomas tal que A, B $\in$ Mod($\Gamma$) $\Rightarrow$ A $\cong$ B. Os Teoremas de Skolem–Löwenheim têm nos ensinado que isso é (exceto para o caso finito) inatingível. Há, no entanto, uma noção significativa:

**Definição 3.3.15** Seja $\kappa$ um cardinal. Uma teoria é $\kappa$-categórica se ela tem no mínimo um modelo de cardinalidade $\kappa$ e se quaisquer dois modelos de cardinalidade $\kappa$ são isomorfos.

Categoricidade em alguma cardinalidade não é tão incomum quanto se poderia pensar. Enumeramos alguns exemplos.

1. *A teoria dos conjuntos infinitos (estruturas de identidade) é $\kappa$-categórica para todo $\kappa$ infinito.*

*Demonstração.* Imediata, porque aqui "isomorfo" significa "de mesma cardinalidade". ☐

2. *A teoria dos conjuntos densamente ordenados sem extremos é $\aleph_0$-categórica.*

*Demonstração.* Veja em qualquer livro texto sobre teoria dos conjuntos. O teorema foi demonstrado por Cantor usando o chamado método ida-e-volta. ☐

3. *A teoria dos grupos abelianos livres-de-torsão divisíveis é $\kappa$-categórica para $\kappa > \aleph_0$.*

*Demonstração.* Verifique que um grupo abeliano livre-de-torsão divisível é um espaço vetorial sobre os racionais. Use o fato de que espaços vetoriais de mesma dimensão (sobre o mesmo corpo) são isomorfos. ☐

4. *A teoria dos corpos algebricamente fechados (de uma característica fixa) é $\kappa$-categórica para $\kappa > \aleph_0$.*

*Demonstração.* Use o Teorema de Steinitz: dois corpos algebricamente fechados de mesma característica e de mesmo grau incontável de transcendência são isomorfos. ☐

A conexão entre categoricidade e completude, para linguagens contáveis, é dada por

**Teorema 3.3.16 (Teorema de Vaught)** *Se $T$ não tem modelos finitos e é $\kappa$-categórica para algum $\kappa$ que não é menor que a cardinalidade de $L$, então $T$ é completa.*

*Demonstração.* Suponha que $T$ não seja completa. Então existe uma $\sigma$ tal que $T \nvdash \sigma$ e $T \nvdash \neg\sigma$. Pelo Lema da Existência de Modelo, existem $\mathrm{A}$ e $\mathrm{B}$ em $\mathrm{Mod}(T)$ tais que $\mathrm{A} \models \sigma$ e $\mathrm{B} \models \neg\sigma$. Como $\mathrm{A}$ e $\mathrm{B}$ são infinitos podemos aplicar o Teorema de Skolem–Löwenheim (de-cima-para-baixo ou de-baixo-para-cima), de modo a obter $\mathrm{A}'$ e $\mathrm{B}'$, de cardinalidade $\kappa$, tais que $\mathrm{A} \equiv \mathrm{A}'$, e $\mathrm{B} \equiv \mathrm{B}'$. Mas então $\mathrm{A}' \equiv \mathrm{B}'$, e portanto $\mathrm{A}' \equiv \mathrm{B}'$, logo $\mathrm{A} \equiv \mathrm{B}$.

Isso contradiz o fato de que $\mathrm{A} \models \sigma$ e $\mathrm{B} \models \neg\sigma$. ☐

Como conseqüência vemos que as seguintes teorias são completas:

1. a teoria dos conjuntos infinitos;
2. a teoria dos conjuntos densamente ordenados sem extremos;
3. a teoria dos grupos abelianos livres-de-torsão divisíveis;

4. a teoria dos corpos algebricamente fechados de característica fixa.

Um corolário do último fato ficou conhecido como *princípio de Lefschetz*: *se uma sentença $\sigma$, na linguagem de primeira ordem dos corpos, se verifica para todos os números complexos, ela se verifica para todos os corpos algebricamente fechados de característica zero.*

Isso significa que um teorema "algébrico" $\sigma$ sobre corpos algebricamente fechados de característica 0 pode ser obtido através da concepção de uma prova por quaisquer que sejam os meios (analíticos, topológicos, ...) para o caso especial dos números complexos.

**Decidibilidade.**

Vimos no Capítulo 1 que existe um método efetivo para se testar se uma proposição é demonstrável – por meio da técnica da tabela-verdade, pois "verdade = demonstrabilidade".

Seria maravilhoso dispor um tal método para a lógica de predicados. Church mostrou, no entanto, que não existe tal método (se entendermos "efetivo" como "recursivo") para a lógica geral de predicados. Mas poderia haver, e de fato existem, teorias especiais que são decidíveis. Um estudo técnico de decidibilidade faz parte da teoria da recursão. Aqui apresentaremos algumas poucas considerações.

Se $T$, com linguagem $L$, tem um conjunto decidível de axiomas $\Gamma$, então existe um método efetivo de enumerar todos os teoremas de $T$.

Pode-se obter tal enumeração da seguinte maneira:

(a) Construa uma lista efetiva $\sigma_1, \sigma_2, \sigma_3, \ldots$ de todos os axiomas de $T$ (isso é possível porque $\Gamma$ é decidível), e uma lista $\varphi_1, \varphi_2, \ldots$ de todas as fórmulas de $L$.

(b)

   (1) escreva todas as derivações de tamanho 1, usando $\sigma_1, \varphi_1$, com no máximo $\sigma_1$ não cancelada,

   (2) escreva todas as derivações de tamanho 2, usando $\sigma_1, \sigma_2, \varphi_1, \varphi_2$, com no máximo $\sigma_1, \sigma_2$ não canceladas,

   $\vdots$

   ($n$) escreva todas as derivações de tamanho $n$, usando $\sigma_1, \ldots, \sigma_n, \varphi_1, \ldots, \varphi_n$, com no máximo $\sigma_1, \ldots, \sigma_n$ não canceladas,

   $\vdots$

A cada vez obtemos apenas um número finito de teoremas e cada teorema é derivado em algum momento. O processo é claramente efetivo (embora não eficiente).

Agora observamos

**Lema 3.3.17** *Se $\Gamma$ e $\Gamma^c$ (o complemento de $\Gamma$) são efetivamente enumeráveis, então $\Gamma$ é decidível.*

*Demonstração.* Gere as listas de $\Gamma$ e $\Gamma^c$ simultaneamente. Em um número finito de passos encontraremos $\sigma$ na lista de $\Gamma$ ou na lista de $\Gamma^c$. Logo para cada $\sigma$ podemos decidir em um número finito de passos se $\sigma \in \Gamma$ ou não. □

Como um corolário obtemos o

**Teorema 3.3.18** *Se $T$ é efetivamente axiomatizável e completa, então $T$ é decidível.*

*Demonstração.* Como $T$ é completa, temos que $\Gamma \vdash \sigma$ ou $\Gamma \vdash \neg\sigma$ para cada $\sigma$ (onde $\Gamma$ axiomatiza $T$). Logo $\sigma \in T^c \Leftrightarrow \Gamma \not\vdash \sigma \Leftrightarrow \Gamma \vdash \neg\sigma$.
Do esboço acima segue que $T$ e $T^c$ são efetivamente enumeráveis. Pelo lema $T$ é decidível. □

*Aplicação.* As seguintes teorias são decidíveis:

1. a teoria dos conjuntos infinitos;
2. a teoria dos conjuntos densamente ordenados sem extremos;
3. a teoria dos grupos abelianos livres-de-torsão divisíveis;
4. a teoria dos corpos algebricamente fechados de característica fixa.

*Demonstração.* Veja as conseqüências do Teorema de Vaught (3.3.16). A enumeração efetiva é deixada ao leitor (o caso mais simples é, obviamente, aquele em que temos uma teoria finitamente axiomatizável, e.g. (1) ou (2)). □

Apresentaremos finalmente mais uma aplicação da abordagem não-padrão, dando uma demonstração não-padrão de

**Lema 3.3.19 (Lema de König)** *Uma árvore finitária infinita tem um ramo infinito.*

Uma árvore finitária, ou *leque* (em inglês, *fan*), tem a propriedade de que cada nó tem apenas um número finito de sucessores imediatos ('zero sucessores' está incluído). Por contraposição obtém-se a partir do Lema de König o chamado *Teorema do Leque* (em inglês, *Fan Theorem*) (que na verdade foi descoberto primeiro):

**Teorema 3.3.20** *Se em um leque todos os ramos são finitos então o comprimento dos ramos é limitado.*

Note que se se considera a árvore como um espaço topológico, com sua topologia canônica (conjuntos abertos básicos "são" nós), então o Lema de König é o Teorema de Bolzano–Weierstrasz e o Teorema do Leque enuncia a compaccidade.

Daremos agora uma demonstração não-padrão do Lema de König.

Seja $T$ um leque, e $T^*$ uma extensão elementar própria (use 3.3.13).

(1) a relação "... é um sucessor imediato de ..." pode ser expressa na linguagem da ordem parcial:

$x \leq_i y := x < y \wedge \forall z(x \leq z \leq y \rightarrow x = z \vee y = z)$ onde, como de costume, $x < y$ representa $x \leq y \wedge x \neq y$.

(2) Se $a$ é padrão, então os sucessores imediatos em $T^*$ também são padrão. Como $T$ é finitária, podemos apontar $a_1, \ldots, a_n$ tais que

$T \models \forall x(x <_i \bar{a} \leftrightarrow \bigvee_{1 \leq k \leq n} \bar{a}_k = x)$. Devido a $T \prec T^*$, temos também que

$T^* \models \forall x(x <_i \bar{a} \leftrightarrow \bigvee_{1 \leq k \leq n} \bar{a}_k = x)$, logo se $b$ é um sucessor imediato de $a$ em $T^*$, então $b = a_k$ para algum $k \leq n$, i.e. $b$ é padrão.

Note que um nó sem sucessores em $T$ também não tem sucessores em $T^*$, pois $T \models \forall x(x \leq \bar{a} \leftrightarrow x = \bar{a}) \Leftrightarrow T^* \models \forall x(x \leq \bar{a} \leftrightarrow x = \bar{a})$.

(3) Em $T$ temos que um sucessor de um nó é um sucessor imediato daquele nó ou um sucessor de um sucessor imediato, i.e.

$$T \models \forall xy(x < y \rightarrow \exists z(x \leq z <_i y)).\ (*)$$

Isso é caso pois para nós $a$ e $b$ com $a < b$, $b$ tem que ocorrer na cadeia finita de todos os predecessores de $a$. Logo faça $a = a_n < a_{n-1} < \ldots < a_i = b < a_{i-1} < \ldots$, então $a \leq a_{i+1} <_i b$.

Como a propriedade desejada é expressa por uma sentença de primeira ordem $(*)$, (3) também se verifica em $T^*$.

(4) figura pagina 130

Seja $a^*$ um elemento não-padrão de $T^*$. Alegamos que

$P = \{a \in |T| \mid a^* < a\}$ é um ramo infinito (i.e. uma cadeia).

(i) $P$ é linearmente ordenado pois $T \models \forall xyz(x \leq y \wedge x \leq z \rightarrow y \leq z \vee z \leq y)$ e portanto para qualquer $p, q \in P \in P \subseteq |T^*|$ temos que $p \leq q$ ou $q \leq p$.

(ii) Suponha que $P$ seja finito com $b$ como último elemento, então $b$ tem um sucessor e daí um sucessor imediato em $T^*$, que é predecessor de $a^*$.

Pelo item (2) esse sucessor imediato pertence a $P$. Contradição. Daí $P$ é infinito.

Isso estabelece que $T$ tem um ramo infinito. $\square$

**Eliminação de Quantificadores**

Algumas teorias têm a agradável propriedade de que elas permitem a redução de fórmulas a uma forma particularmente simples: uma forma na qual nenhum quantificador ocorre. Sem entrar por uma teoria geral da eliminação de quantificadores, demonstraremos o procedimento em um caso simples: *a teoria $\mathcal{DO}$ das ordens densas sem extremos*, cf. 2.7.3(ii); 'sem extremos' é formulada como "$\forall x \exists yz((y < x \wedge x < z)$".

Seja $VL(\varphi) = \{y_1, \ldots, y_n\}$, onde todas as variáveis realmente ocorrem em $\varphi$. Pelos métodos usuais obtemos uma forma normal prenex $\varphi'$ de $\varphi$, tal que $\varphi' := Q_1 x_1 Q_2 \ldots Q_m x_m \psi(x_1, \ldots, x_m, y_1, \ldots, y_n)$, onde cada $Q_i$ é um dos quantificadores $\forall$ ou $\exists$. Eliminaremos os quantificadores começando com o mais interno.

Considere o caso em que $Q_m = \exists$. Vamos trazer $\psi$ à forma normal disjuntiva $\bigvee \psi_j$, onde cada $\psi_j$ é uma conjunção de átomos e negações de átomos. Primeiro observe que as negações de átomos podem ser eliminadas em favor de átomos, pois $\mathcal{DO} \vdash \neg z = z' \leftrightarrow (z < z' \vee z' < z)$ e $\mathcal{DO} \vdash \neg z < z' \leftrightarrow (z = z' \vee z' < z)$. Portanto podemos assumir que os $\psi_j$'s contêm apenas átomos.

Usando simplesmente lógica de predicados podemos substituir $\exists x_m \bigvee \psi_j$ pela fórmula equivalente $\bigvee \exists x_m \psi_j$.

*Notação:* para o resto deste exemplo usaremos $\psi \overset{*}{\leftrightarrow} \tau$ como uma abreviação para $\mathcal{DO} \vdash \sigma \leftrightarrow \tau$.

Acabamos de ver que basta considerar apenas fórmulas da forma $\exists x_m \bigwedge \sigma_p$, onde cada $\sigma_p$ é atômica. Uma olhada sistemática nos operandos da conjunção nos mostrará o que fazer.

(1) Se $x_m$ não ocorre em $\bigwedge \sigma_p$, podemos apagar os quantificadores (cf. 2.5.2).

(2) Caso contrário, pegue todos os átomos contendo $x_m$ e faça um reagrupamento, tal que obtemos $\bigwedge \sigma_p \overset{*}{\leftrightarrow} \bigwedge_i x_m < u_i \wedge \bigwedge_j v_j < x_m \wedge \bigwedge_k w_k = x_m \wedge \chi$, onde $\chi$ não contém $x_m$. Abrevie essa fórmula como $\tau \wedge \chi$. Pela lógica de predicados temos que $\exists x_m(\tau \wedge \chi) \overset{*}{\leftrightarrow} \exists x_m \tau \wedge \chi$ (cf. 2.5.3). Como desejamos eliminar $\exists x_m$, basta considerar apenas $\exists x_m \tau$.

Agora o problema foi reduzido a um problema de marcação. Imaginando que estamos lidando com uma ordem linear, exploraremos a informação dada por $\tau$ sobre a posição relativa dos $u_i, v_j, w_k$'s com respeito a $x_m$.

(2a) $\tau := \bigwedge x_m < u_i \wedge \bigwedge v_j < x_m \wedge \bigwedge w_k = x_k$.

Então $\exists x_m \tau \overset{*}{\leftrightarrow} \tau'$, com $\tau' := \bigwedge w_0 < u_i \wedge \bigwedge v_j < w_0 \wedge \bigwedge w_0 = w_k$ (onde $w_0$ é a primeira variável entre os $w_k$'s). A equivalência segue imediatamente usando um argumento da teoria dos modelos (i.e. $\mathcal{DO} \models \exists x_m \tau \leftrightarrow \tau'$).

(2b) $\tau := \bigwedge x_m < u_i \wedge \bigwedge v_j < x_m$.

Agora as propriedades de $\mathcal{DO}$ são essenciais. Observe que $\exists x_m(\bigwedge x_m < \bar{a}_i \wedge \bigwedge \bar{b}_j < x_m)$ se verifica em um conjunto *densamente ordenado* se e somente se todos os $a_i$'s estejam à direita dos $b_j$'s. Logo obtemos (por completude) $\exists x_m \tau \overset{*}{\leftrightarrow} \bigwedge_{i,j} v_j < u_i$.

(2c) $\tau := \bigwedge x_m < u_i \wedge \bigwedge w_k = x_m$.

Então $\exists x_m \tau \overset{*}{\leftrightarrow} \bigwedge w_0 < u_i \wedge \bigwedge w_k = w_0$.

(2d) $\tau := \bigwedge v_j < x_m \wedge \bigwedge w_k = x_m$.
Cf. (2c).

(2e) $\tau := \bigwedge x_m < u_i$.

Observe que $\exists x_m \tau$ se verifica em todos os conjuntos ordenados sem um extremo à esquerda. Logo temos que $\exists x_m \overset{*}{\leftrightarrow} \top$, pois trabalhamos em $\mathcal{DO}$.

(2f) $\tau := \bigwedge v_j < x_m$.
Cf. (2e).

(2g) $\tau := \bigwedge w_k = x_m$.

Então $\exists x_m \tau \overset{*}{\leftrightarrow} \bigwedge w_0 = w_k$.

*Observações.*

(i) Os casos (2b), (2e) e (2f) fazem uso de $\mathcal{DO}$.

(ii) Frequentemente é possível introduzir atalhos, e.g. quando uma variável (que não seja $x_m$) ocorre em dois dos grandes operandos da conjunção temos que $\exists x_m \tau \overset{*}{\leftrightarrow} \perp$.

Se o quantificador mais interno é universal, reduzimos a um existencial pela equivalência $\forall x_m \varphi \leftrightarrow \neg \exists x_m \neg \varphi$.

Agora está claro como eliminar os quantificadores um por um.

***Exemplo.***

$$\exists xy(x < y \wedge \exists z(x < z \wedge z < y \wedge \forall u(u \neq z \to u < y \vee u = z)))$$

$$\overset{*}{\leftrightarrow} \quad \exists xyz \forall u(x < y \wedge x < z \wedge z < y \wedge (u = z \vee u < y \vee u = x))$$

$$\overset{*}{\leftrightarrow} \quad \exists xyz \neg \exists u(\neg x < y \vee \neg x < z \vee \neg z < y \vee (\neg u = z \wedge \neg u < y \wedge \neg u = x))$$

$$\begin{aligned} \overset{*}{\leftrightarrow} \quad & \exists xyz \neg \exists u(x = y \vee y < x \vee x = z \vee z < x \vee z = y \vee y < z \vee \\ & ((u < z \vee z < u) \wedge (u = y \vee y < u) \wedge (u < x \vee x < u))) \end{aligned}$$

$$\begin{aligned} \overset{*}{\leftrightarrow} \quad & \exists xyz \neg \exists u(x = y \vee y < x \vee x = z \vee z < x \vee z = y \vee y < z \vee \\ & (u < z \wedge u = y \wedge u < x) \vee (u < z \wedge u = y \wedge x < u) \vee \\ & (u < z \wedge y < u \wedge u < x) \vee (u < z \wedge y < u \wedge x < u) \vee \\ & (z < u \wedge u = y \wedge u < x) \vee (z < u \wedge u = y \wedge x < u) \vee \\ & (z < u \wedge y < u \wedge u < x) \vee (z < u \wedge y < u \wedge x < u)). \end{aligned}$$

$$\begin{aligned} \overset{*}{\leftrightarrow} \quad & \exists xyz \neg (x = y \vee y < x \vee x = z \vee z < x \vee z = y \vee y < z \vee \\ & \exists u(u < z \wedge u = y \wedge u < x) \vee \exists u(u < z \wedge u = y \wedge x < u) \vee \ldots \vee \\ & \exists u(z < u \wedge y < u \wedge x < u)). \end{aligned}$$

$$\begin{aligned} \overset{*}{\leftrightarrow} \quad & \exists xyz \neg (x = y \vee \ldots \vee y < z \vee (y < z \wedge y < x) \vee (y < z \vee \wedge x < y) \\ & \vee (y < z \wedge y < x) \vee (y < z \wedge x < z) \vee (z < y \wedge y < x) \\ & \vee (z < y \wedge x < y) \vee (z < x \wedge y < x) \vee \top). \end{aligned}$$

$$\overset{*}{\leftrightarrow} \quad \exists xyz(\neg \top).$$

$$\overset{*}{\leftrightarrow} \quad \perp.$$

Evidentemente esse exemplo de eliminação de quantificadores para a teoria da classe densa sem extremos provê uma demonstração alternativa de sua decidibilidade. Pois, se $\varphi$ é uma sentença, então $\varphi$ é equivalente a uma sentença aberta $\varphi'$. Dada a linguagem de $\mathcal{DO}$ é óbvio que $\varphi'$ é equivalente a $\top$ ou $\perp$. Daí, temos um algoritmo para decidir $\mathcal{DO} \vdash \varphi$. NOte que obtemos mais: $\mathcal{DO}$ é completa, pois $\mathcal{DO} \vdash \varphi \leftrightarrow \perp$ ou $\mathcal{DO} \vdash \leftrightarrow \top$, logo $\mathcal{DO} \vdash \neg\varphi$ ou $\mathcal{DO} \vdash \varphi$.

Em geral não podemos esperar tanto da eliminação de quantificadores: e.g. a teoria dos corpos algebricamente fechados admite eliminação de quantificadores, mas não é completa (porque a característica não foi fixada com antecipação); as sentenças abertas podem conter átomos indemonstráveis e irrefutáveis tais como $7 = 12$, $23 = 0$.

Podemos concluir da existência de uma eliminação de quantificadores uma certa propriedade segundo a teoria dos modelos, introduzida por Abraham Robinson, que tornou-se importante para aplicações em álgebra (cf. o *Handbook of Mathematical Logic*, $A_4$).

**Definição 3.3.21** Uma teoria $T$ é *modelo completa* se para $\mathrm{A}, \mathrm{B} \in \mathrm{Mod}(T)$ $\mathrm{A} \subseteq \mathrm{B} \Rightarrow \mathrm{A} \prec \mathrm{B}$.

**Teorema 3.3.22** *Se $T$ admite eliminação de quantificadores, então $T$ é modelo completa.*

*Demonstração.* Sejam A e B modelos de $T$, tais que $\mathrm{A} \subseteq \mathrm{B}$. Temos que mostrar que $\mathrm{A} \models \varphi(\overline{a}_1, \ldots, \overline{a}_n) \Leftrightarrow \mathrm{B} \models \varphi(\overline{a}_1, \ldots, \overline{a}_n)$ para todos $a_1, \ldots, a_n \in |\mathrm{A}|$, onde $VL(\varphi) = \{x_1, \ldots, x_n\}$.

Como $T$ admite eliminação de quantificadores, existe uma fórmula livre-de-quantificadores $\psi(x_1, \ldots, x_n)$ tal que $\Gamma \vdash \varphi \leftrightarrow \psi$.

Daí basta mostrar que $\mathrm{A} \models \psi(\overline{a}_1, \ldots, \overline{a}_n) \Leftrightarrow \mathrm{B} \models \psi(\overline{a}_1, \ldots, \overline{a}_n)$ para uma fórmula livre-de-quantificador $\psi$. Uma indução simples estabelece essa equivalência.

Algumas teorias $T$ têm um modelo especial que está, a menos de isomorfismo, contido em todo modelo de $T$. Chamamos tal modelo de um *modelo primo* de $T$.

*Exemplos.*

(i) Os racionais formam um modelo primo para a teoria da ordenação densa sem extremos;

(ii) O corpo dos racionais é o modelo primo da teoria dos corpos de característica zero;

(iii) O modelo padrão da aritmética é o modelo primo da aritmética de Peano.

**Teorema 3.3.23** *Uma teoria modelo completa com um modelo primo é completa.*

*Demonstração.* Deixo ao leitor. □

**Exercícios**

1. Seja $\mathrm{A} = \langle A, < \rangle$ um conjunto parcialmente ordenado. Mostre que $\mathrm{Diag}^+(\mathrm{A}) \cup \{\overline{a} \neq \overline{b} \mid a \neq b, a, b \in |\mathrm{A}|\} \cup \{\forall xy(x \leq y \vee y \leq x)\}$ tem um modelo. (Sugestão: use compaccidade.)

   Conclua que todo conjunto parcialmente ordenado pode ser linearmente ordenado por uma ordem que é uma extensão de sua ordenação.

2. (i) Um grupo pode ser ordenado $\Leftrightarrow$ cada subgrupo finitamente gerado pode ser ordenado. (Sugestão: Olhe para $\mathrm{Diag}(\mathrm{A}) \cup \Gamma$, onde $\Gamma$ é o conjunto de axiomas da teoria dos grupos ordenados.)

   (ii) Um grupo abeliano A pode ser ordenado $\Leftrightarrow$ A é livre de torsão. (Sugestão: como no caso anterior. Use o fato de que um grupo abeliano livre de torsão finitamente gerado é isomorfo a alguma potência de $\mathbb{Z}$, cf. Lang, *Algebra*.

3. Um grafo (com $R$ simétrica e irreflexiva) é chamado de $k$-colorível se podemos pintar os vértices com $k$ cores diferentes tal que vértices adjacentes tenham cores distintas. Formulamos isso adicionando $K$ predicados unários $C_1, \ldots, C_k$, mais os seguintes axiomas

$$\forall x \bigvee_i C_i(x), \bigwedge_{i \neq j} \neg(C_i(x) \wedge C_j(x)),$$

$$\bigwedge_i \forall xy(C_i(x) \wedge C_i(y) \rightarrow \neg R(x, y)).$$

   Mostre que um grafo é $k$-colorível se cada subgrafo finito é $k$-colorível (De Bruijn–Erdös).

4. Se $f : \mathrm{A} \rightarrow \mathrm{B}$ e $VL(\varphi) = \{x_1, \ldots, x_n\}$, mostre que $\mathrm{A} \vdash \varphi[\overline{a}_1, \ldots, \overline{a}_n / x_1, \ldots, x_n] \Leftrightarrow \mathrm{B} \vdash\vdash \varphi[\overline{f(a_1)}, \ldots, \overline{f(a_n)} / x_1, \ldots, x_n]$.

   Em particular, $\mathrm{A} \equiv \mathrm{B}$.

5. Seja $\mathrm{A} \subseteq \mathrm{B}$. $\varphi$ ćhamada de *universal* (*existencial*) se $\varphi$ está na forma prenex com apenas quantificadores universais (existenciais).

   (i) Mostre que para toda sentença universal $\varphi$, $\mathrm{B} \models \varphi \Rightarrow \mathrm{A} \models \varphi$.

   (ii) Mostre que para toda sentença existencial $\varphi$, $\mathrm{A} \models \varphi \Rightarrow \mathrm{B} \models \varphi$.

   (Aplicação: uma subestrutura de um grupo é um grupo. Essa é uma razão para usar o tipo de similaridade $\langle -; 2, 1; 1 \rangle$ para grupos, ao invés de $\langle -; 2; 0 \rangle$, ou $\langle -; 2; 1 \rangle$, como alguns autores fazem).

6. Seja $\mathrm{A} = \langle N, < \rangle$, e $\mathrm{B} = \langle N - \{0\}, < \rangle$.

   Mostre que:

| | | | |
|---|---|---|---|
| (i) | $\mathrm{A} \cong \mathrm{B}$ | (ii) | $\mathrm{A} \equiv \mathrm{B}$; |
| (iii) | $\mathrm{B} \subseteq \mathrm{A}$ | (iv) | não é verdade que $\mathrm{B} \prec \mathrm{A}$. |

7. (Tarski). Seja $\mathrm{A} \subseteq \mathrm{B}$. Mostre que $\mathrm{A} \prec \mathrm{B} \Leftrightarrow$ para toda $\varphi \in L$ e $a_1, \ldots, a_n \in |\mathrm{A}|$, $\mathrm{B} \vdash \exists y \varphi(y, \overline{a}_1, \ldots, \overline{n}) \Rightarrow$ existe um elemento $a \in |\mathrm{A}|$ tal que $\mathrm{B} \vdash \varphi(\overline{a}, \overline{a}_1, \ldots, \overline{a}_n)$, onde $VL(\varphi(y, \overline{a}_1, \ldots, \overline{a}_n) = \{y\}$. Sugestão: para $\Leftrightarrow$ mostre que

   (i) $t^{\mathrm{A}}(\overline{a}_1, \ldots, \overline{a}_n) = t^{\mathrm{B}}(\overline{a}_1, \ldots, \overline{a}_n)$ para $t \in L$,

   (ii) $\mathrm{A} \vdash \varphi(\overline{a}_1, \ldots, \overline{a}_n) \Leftrightarrow \mathrm{B} \vdash \varphi(\overline{a}_1, \ldots, \overline{a}_n)$ para $\varphi \in L$ por indução sobre $\varphi$ (use apenas $\vee, \neg, \exists$).

8. Uma outra construção de um modelo não-padrão da aritmética: Adicione à linguagem $L$ da aritmética uma nova constante $c$. Mostre que $\Gamma = \mathrm{Th}(\hat{\mathrm{N}}) \cup \{c > \overline{\phantom{n}}n \in |\mathrm{N}|\}$ tem um modelo M. Mostre que $\mathrm{M} \not\cong \mathrm{N}$. M pode ser contável?

9. Considere o anel $Z$ dos inteiros. Mostre que existe uma estrutura A tal que $Z \prec \mathrm{A}$ e $Z \not\cong \mathrm{A}$ (um modelo não-padrão dos inteiros). Mostre que A tem um "número primo infinito", $p_\infty$.

Seja $(p_\infty)$ o ideal principal em A gerado por $p_\infty$. Mostre que $\mathrm{A}/(p_\infty)$ é um corpo $F$. (Sugestão: olhe em $\forall x($"$x$ não pertence a $(p_\infty)$"$\to \exists yz(xy = 1 + zp_\infty))$, dê uma formulação propriamente dita e use equivalência elementar). Qual é a característica de $F$? (Isso dá origem a uma construção não-padrão dos racionais a partir dos inteiros: considere o corpo primo).

10. Use o modelo não-padrão da aritmética para mostrar que "boa-ordenação" não é um conceito de primeira ordem.

11. Use o modelo não-padrão da aritmética para mostrar que "corpo ordenado arquimedeano" não é um conceito de primeira ordem.

12. Considere a linguagem da identidade com constantes $c_i$ $(i \in N)$

    $\Gamma = \{I_1, I_2, I_3\} \cup \{c_i \neq c_j \mid i, j \in N, i \neq j\}$. Mostre que a teoria de $\Gamma$ é $\kappa$-categórica para $\kappa > \aleph_0$, mas não $\aleph_0$-categórica.

13. Mostre que a condição "nenhum modelo finito" no Teorema de Vaught é necessária (olhe a teoria da identidade).

14. Seja $X \subseteq |\mathrm{A}|$. Defina $X_0 = X \cup C$ onde $C$ é o conjunto de constantes de A, $X_{n+1} = X_n \cup \{f(b_1, \ldots, b_m) \mid f \text{ em } \mathrm{A}, b_1, \ldots, b_m \in X_n\}$, $X_\omega = \bigcup\{X_n \mid n \in \mathbb{N}\}$.

    Mostre que: $\mathrm{B} = \langle X_\omega, R_1 \cap X_\omega^{r_1}, \ldots, R_n \cap X_\omega^{r_n}, f_1|X_\omega^{a_1}, \ldots, f_m|X_\omega^{a_m}, \{c_i \mid i \in I\}\rangle$ é uma subestrutura de A. Dizemos que B é a subestrutura gerada por $X$. Mostre que B é a menor subestrutura de A contendo $X$; B também pode ser caracterizada como a interseção de todas as subestruturas contendo $X$.

15. Seja ${}^*R$ um modelo não-padrão de $\mathrm{Th}(R)$. Mostre que *pad* (cf. Aplicação II, após o Lema do Transbordamento) é um homomorfismo do anel dos números finitos para $R$. Qual é o *kernel*?

16. Considere $\mathrm{R}' = \langle R, N, <, +, \cdot, -, ^{-1}, 0, 1\rangle$, onde $N$ é o conjunto dos números naturais. $L(\mathrm{R}')$ tem o símbolo de predicado $N$ e, caso nos limitemos a $+$ e $\cdot$, podemos recuperar a aritmética relativizando nossas fórmulas a $N$ (cf. 2.5.9).

    Seja $\mathrm{R}' \prec {}^*\mathrm{R}' = \langle {}^*R, {}^*N, \ldots\rangle$. Mostre que $\mathrm{N} = \langle N, <, +, \cdot, 0, 1\rangle \prec \langle {}^*N, <, +, \cdot, 0, 1\rangle = {}^*\mathrm{N}$ (Sugestão: considere para cada $\varphi \in L(\mathrm{R})$ a fórmula relativizada $\varphi^N \in L(\mathrm{R}')$).

17. Mostre que qualquer estrutura de Peano contém N como uma subestrutura.

18. Seja $L$ uma linguagem sem a identidade e com no mínimo uma constante. Seja $\sigma = \exists x_1 \ldots x_n \varphi(x_1, \ldots, x_n)$ e $\Sigma_s igma = \{\varphi(t_1, \ldots, t_n) \mid t_i \text{ fechado em } L\}$, onde $\varphi$ é livre de quantificador.

    (i) $\models \sigma \Leftrightarrow$ cada A é um modelo de no mínimo uma sentença em $\Sigma_\sigma$. (Sugestão: para cada A, veja a subestrutura gerada por $\emptyset$).

    (ii) Considere $\Sigma_\sigma$ como um conjunto de proposições. Mostre que para cada valoração $v$ (no sentido da lógica proposicional) existe um modelo A tal que $[\![\varphi(t_1, \ldots, t_n)]\!]_v = [\![\varphi(t_1, \ldots, t_n)]\!]_{\mathrm{A}}$, para toda $\varphi(t_1, \ldots, t_n) \in \Sigma_\sigma$.

(iii) Mostre que $\vdash \sigma \Leftrightarrow \bigvee_{i=1}^{m} \varphi(t_1^i, \ldots, t_n^i)$ para um certo $m$ (sugestão: use o Exercício 9, seção 1.5).

19. Sejam $\mathrm{A}, \mathrm{B} \in \mathrm{Mod}(T)$ e $\mathrm{A} \equiv \mathrm{B}$. Mostre que $\mathrm{Diag}(\mathrm{A}) \cup \mathrm{Diag}(\mathrm{B}) \cup T$ é consistente (use o Teorema da Compaccidade). Conclua que existe um modelo de $T$ no qual ambas A e B podem ser isomorficamente imersas, dizemos que A e B têm uma "imersão conjunta".

20. Considere a classe $\mathcal{K}$ de todas as estruturas de tipo $\langle 1; -; 0\rangle$ com uma relação unária enumerável. Mostre que quaisquer A e B em $\mathcal{K}$ de mesma cardinalidade são isomorfas. Mostre que $T = \mathrm{Th}(\mathcal{K})$ não é $\kappa$-categórica para qualquer que seja $\kappa \geq \aleph_0$.

21. Considere uma teoria $T$ da identidade com axiomas $\lambda_n$ para todo $n \in N$. Em quais cardinalidades $T$ é categórica? Mostre que $T$ é completa e decidível. Compare o resultado com o o resultado do Exercício 12.

22. Mostre que a teoria da ordem densa sem extremos não é categórica na cardinalidade do contínuo.

23. Considere a estrutura $\mathrm{A} = \rangle \mathbb{R}, <, f\rangle$, onde $<$ é a ordem natural, e $f$ é uma função unária. Seja $L$ a linguagem correspondente. Mostre que não existe qualquer sentença $\sigma$ de $L$ tal que $\mathrm{A} \models \sigma \Leftrightarrow f(r) > 0$ para todo $r \in R$. (sugestão: considere isomorfismos $x \mapsto x + k$).

24. Seja $\mathrm{A} = \langle A, \sim\rangle$, onde $\sim$ é uma relação de equivalência com uma quantidad enumerável de classes de equivalência, todas as quais infinitas. Mostre que $\mathrm{Th}(\mathrm{A})$ é $\aleph_0$-categórica. Axiomatize $\mathrm{Th}(\mathrm{A})$. Existe uma axiomatização finita? $\mathrm{Th}(\mathrm{A})$ é $\kappa$-categórica para $\kappa > \aleph_0$?

25. Seja $L$ uma linguagem com um símbolo unário de função $f$. Encontre uma sentença $\tau_n$, que diz que "$f$ tem um laço de comprimento $n$", i.e. $\mathrm{A} \models \tau_n \Leftrightarrow$ existem $a_1, \ldots, a_n \in |\mathrm{A}$ tais que $f^{\mathrm{A}}(a_i) = a_{i+1}$ $(i < n)$ e $f^{\mathrm{A}}(a_n) = a_1$. Considere a teoria $T$ com o conjunto de axiomas $\{\beta, \neg\tau_1, \neg\tau_2, \neg\tau_3, \ldots, \neg\tau_n, \ldots\}$ $(n \in \omega)$, onde $\beta$ expressa que "$f$ é bijetora".

    Mostre que $T$ é $\kappa$-categórica para $\kappa > \aleph_0$. (Sugestão: considere a partição $\{(f^{\mathrm{A}})^i(a) \mid i \in \omega\}$ em um modelo A). $T$ é $\aleph_0$-categórica?

    Mostre que $T$ é completa e decidível. $T$ é finitamente axiomatizável?

26. Faça $T_\forall = \{\sigma \mid T \vdash \sigma \text{ e } \sigma \text{ é universal}\}$. Mostre que $T_\forall$ axiomatiza a teoria de todas as subestruturas de modelos de $T$. Note que uma parte segue do Exercício 5. Para a recíproca: seja A um modelo de $T_\forall$ e considere $\mathrm{Diag}(\mathrm{A} \cup T$. Use a compaccidade.

27. Dizemos que uma teoria é *preservada sob subestruturas* se $\mathrm{A} \subseteq \mathrm{B}$ e $\mathrm{B} \in \mathrm{Mod}(T)$ implica $\mathrm{A} \in \mathrm{Mod}(T)$.

    (Loś–Tarski). Mostre que $T$ é preservada sob subestruturas sse $T$ pode ser axiomatizada por sentenças universais (use o Exercício 26).

28. Seja $\mathfrak{A} \equiv \mathfrak{B}$. Mostre que existe uma estrutura $\mathfrak{C}$ tal que $\mathfrak{A} \prec \mathfrak{C}$, $\mathfrak{B} \prec \mathfrak{C}$ (a menos de isomorfismo). Sugestão: assuma que o conjunto das constantes novas de $\hat{\mathfrak{B}}$ é disjunto do conjunto das constantes novas de $\hat{\mathfrak{A}}$. Mostre que $Th(\hat{\mathfrak{A}}) \cup Th(\hat{\mathfrak{B}})$ tem um modelo.

29. Mostre que a ordenação $<$, definida por $x < y := \exists u(y = x + Su)$ é demonstravelmente transitiva na Aritmética de Peano, i.e. $\mathbf{PA} \vdash \forall xyz(x < y \wedge y < z \rightarrow x < z)$.

30. Mostre que
    - (i) $\mathbf{PA} \vdash \forall x(0 \leq x)$ (use indução sobre $x$),
    - (ii) $\mathbf{PA} \vdash \forall x(x = 0 \vee \exists y(y = Sy))$ (use indução sobre $x$),
    - (iii) $\mathbf{PA} \vdash \forall xy(x + y = y + x)$,
    - (iv) $\mathbf{PA} \vdash \forall y(x < y \rightarrow Sx \leq y)$ (use indução sobre $y$),
    - (v) $\mathbf{PA} \vdash \forall xy(x < y \vee x = y \vee y < x)$ (use indução sobre $x$, o caso em que $x = 0$ é simples, e para o passo de $x$ para $Sx$ use (iv)),
    - (vi) $\mathbf{PA} \vdash \forall \neg \exists (y < x \wedge x < Sy)$ (compare com o item (iv)).

31. (i) Mostre que a teoria $L_\infty$ com "universo infinito" (cf. seção 3.1, Exercício 3 ou Exercício 21 acima) admite eliminação de quantificadores.

    (ii) Mostre que $L_\infty$ tem um modelo primo.

## 3.4 Funções de Skolem ou Como Enriquecer Sua Linguagem

Em argumentos matemáticos é comum se encontrar passagens como "....existe um $x$ tal que $\varphi(x)$ se verifica. Seja $a$ tal elemento, então vemos que ...". Em termos de nossa lógica, isso leva à introdução de uma constante sempre que a existência de algum elemento satisfazendo a certa condição tenha sido estabelecida. O problema é que: dessa forma se está fortalecendo a linguagem de uma maneira essencial? Formulando mais precisamente: suponha que $T \vdash \exists x\varphi(x)$. Introduza uma constante (nova) $a$ e substitua $T$ por $T' = T \cup \{\varphi(a)\}$. Pergunta: $T'$ é conservativa sobre $T$, i.e. será que $T' \vdash \psi \Rightarrow T \vdash \psi$ se verifica, para $\psi$ não contendo $a$? Já lidamos com um problema semelhante no contexto de teorias de Henkin (seção 3.1), portanto podemos usar a experiência adquirida naquela ocasião.

**Teorema 3.4.1** *Seja $T$ uma teoria com linguagem $L$, tal que $T \vdash \exists x\varphi(x)$, onde $VL(\varphi) = \{x\}$, e seja $c$ uma constante que não ocorre em $L$. Então $T \cup \{\varphi(c)\}$ é conservativa sobre $T$.*

*Demonstração.* Pelo Lema 3.1.7, $T' = T \cup \{\exists x\varphi(x) \rightarrow \varphi(c)\}$ é conservativa sobre $T$. Se $\psi \in L$ e $T' \cup \{\varphi(c)\} \vdash \psi$, então $T' \cup \{\exists x\varphi(x)\} \vdash \psi$, ou $T' \vdash \exists x\varphi(x) \rightarrow \psi$. Como $T'$ é conservativa sobre $T$ temos que $T \vdash \exists x\varphi(x) \rightarrow \psi$. Usando $T \vdash \exists x\varphi(x)$, obtemos $T \vdash \psi$. (Para uma demonstração alternativa veja o Exercício 6). $\square$

O teorema acima é um caso especial de uma prática muito comum; se, no processo de se demonstrar um teorema, se estabelece que "para cada $x$ existe um $y$ tal que $\varphi(x, y)$", então é conveniente introduzir uma função auxiliar $f$ que pega um $y$ para cada $x$, tal que $\varphi(x, f(x))$ se verifica para cada $x$. Essa técnica usualmente envolve o axioma da escolha. Podemos fazer a mesma pergunta nesse caso: se $T \vdash \forall x \exists y \varphi(x, y)$, introduza um símbolo de função $f$ e substitua $T$ por $T' = T \cup \{\forall x \varphi(x, f(x))\}$. Pergunta: $T'$ é conservativa sobre $T$? A idéia de enriquecer a linguagem através da introdução de símbolos adicionais de função, que fazem o papel de funções de escolha, remonta a Skolem.

**Definição 3.4.2** Seja $\varphi$ uma fórmula da linguagem $L$ com $VL(\varphi) = \{x_1, \ldots, x_n, y\}$. Associe a $\varphi$ um símbolo $n$-ário de função $f_\varphi$ chamado de *(símbolo de) função de Skolem*. A sentença

$$\forall x_1 \ldots x_n (\exists y \varphi(x_1, \ldots, x_n, y) \to \varphi(x_1, \ldots, x_n, f_\varphi(x_1, \ldots, x_n)))$$

é chamada de *axioma de Skolem* para $\varphi$.

Note que a testemunha da seção 3.1 é um caso especial de uma função de Skolem (tome $n = 0$): $f_\varphi$ é uma constante.

**Definição 3.4.3** Se $T$ é uma teoria com linguagem $L$, então $T^{sk} = T \cup \{\sigma \mid \sigma$ é um axioma de Skolem para alguma fórmula de $L\}$ é a extensão de Skolem de $T$ e sua linguagem $L^{sk}$ estende-se para $L$ através da inclusão de todas as funções de Skolem para $L$. Se A é do tipo de $L$ e $\mathrm{A}^{sk}$ uma expansão de A do tipo de $L^{sk}$, tal que $\mathrm{A}^{sk} \models \sigma$ para todos os axiomas de Skolem de $L$ e $|\mathrm{A}| = |\mathrm{A}^{sk}|$, então $\mathrm{A}^{sk}$ é chamada de uma *expansão de Skolem* de A.

A interpretação em $\mathrm{A}^{sk}$ de um símbolo de função de Skolem é chamada de uma função de Skolem.

Note que uma expansão de Skolem contém uma quantidade infinita de funções, portanto ela é uma suave extensão de noção de estrutura. O análogo de 3.1.7 é

**Teorema 3.4.4** (i) *$T^{sk}$ é conservativa sobre $T$.*
(ii) *Cada* $\mathrm{A} \in \mathrm{Mod}(T)$ *tem uma expansão de Skolem* $\mathrm{A}^{sk} \in \mathrm{Mod}(T^{sk})$.

*Demonstração*. Primeiro mostramos (ii). Consideramos apenas o caso de fórmulas com $VL(\varphi) = \{x_1, \ldots, x_n, y\}$ para $n \geq 1$. O caso em que $n = 0$ é semelhante, porém mais simples. Ele requer a introdução de novas constantes em A (cf. Exercício 6). Suponha que $\mathrm{A} \in \mathrm{Mod}(T)$ e $\varphi \in L$ com $VL(\varphi) = \{x_1, \ldots, x_n, y\}$. Queremos encontrar uma função de Skolem para $\varphi$ em A.

Defina $V_{a_1,\ldots,a_n} = \{b \in |\mathrm{A}| \mid \mathrm{A} \models \varphi(\overline{a}_1, \ldots, \overline{a}_n, \overline{b})\}$.

Aplique $AE$, o axioma da escolha, ao conjunto $\{V_{a_1,\ldots,a_n} \mid V_{a_1,\ldots,a_n} \neq \emptyset\}$: existe uma função de escolha $F$ tal que $F(V_{a_1,\ldots,a_n}) \in V_{a_1,\ldots,a_n}$.

Defina uma função de Skolem por

$$F_\varphi(a_1, \ldots, a_n) = \begin{cases} F(V_{a_1,\ldots,a_n}) & \text{se } V_{a_1,\ldots,a_n} \neq \emptyset, \\ e & \text{caso contrário} \end{cases}$$

onde $e \in |\mathrm{A}|$.

Agora é uma questão de rotina verificar que de fato $\mathrm{A}^{sk} \models \forall x_1 \ldots x_n (\exists y \varphi(x_1, \ldots, x_n, y) \to \varphi(x_1, \ldots, x_n, f_\varphi(x_1, \ldots, x_n)))$, onde $F_\varphi = f_\varphi^{\mathrm{A}^{sk}}$, e $\mathrm{A}^{sk}$ é a expansão de A com todas as funções de Skolem $F_\varphi$ (incluindo as "constantes de Skolem", i.e. testemunhas). O item (i) segue imediatamente do item (ii): Seja $T \not\vdash \psi$ (com $\psi \in L$), então existe uma estrutura A tal que $\mathrm{A} \not\models \psi$. Como $\psi \in L$, temos também que $\mathrm{A}^{sk} \not\models \psi$ (cf. seção 3.2, Exercício 3), daí $T^{sk} \not\vdash \psi$. □

*Observação.* Não é necessário (devido a 3.4.4) estender $L$ com *todas* os símbolos de função de Skolem. Podemos adicionar somente símbolos de função para algum conjunto dado $S$ de fórmulas de $L$. Falamos então da extensão de Skolem de $T$ com respeito a $S$ (ou com respeito a $\varphi$ se $S = \{\varphi\}$).

O seguinte corolário confirma que podemos introduzir funções de Skolem no curso de um argumento matemático, sem fortalecer essencialmente a teoria.

**Corolário 3.4.5** *Se $T \vdash \forall x_1 x_n \exists y \varphi(x_1, \ldots, x_n, y)$ onde $VL(\varphi) = \{x_1, \ldots, x_n, y\}$, então $T' = T \cup \{\forall x_1 \ldots x_n \varphi(x_1, \ldots, x_n, f(x_1, \ldots, x_n))\}$ é conservativa sobre $T$.*

*Demonstração.* Observe que $T'' = T \cup \{\forall x_1 \ldots x_n (\exists y \varphi(x_1, \ldots, x_n, y) \rightarrow \varphi(x_1, \ldots, x_n, f(x_1, \ldots, x_n)) \vdash \forall x_1 \ldots x_n \varphi(x_1, \ldots, x_n, f_\varphi(x_1, \ldots, x_n))$. Logo $T' \vdash \psi \Rightarrow T'' \vdash \psi$. Agora aplique 3.4.4. $\square$

A introdução de uma extensão de Skolem de uma teoria $T$ resulta na “eliminação” do quantificador existencial que ocorre em prefixos da forma $\forall x_1 \ldots x_n \exists y$. A iteração desse processo sobre as formas normais prenex acaba resultando na eliminação de todos os quantificadores existenciais.

As funções de Skolem em um modelo expandido não são de forma alguma únicas. Se, no entanto, $\mathrm{A} \models \forall x_1 \ldots x_n \exists! y \varphi(x_1, \ldots, x_n, y)$, então a função de Skolem para $\varphi$ é unicamente determinada; temos inclusive $\mathrm{A}^{sk} \models \forall x_1 \ldots x_n y(\varphi(x_1, \ldots, x_n, y) \leftrightarrow y = f_\varphi(x_1, \ldots, x_n))$.

Dizemos que $\varphi$ *define* a função $F_\varphi$ em $\mathrm{A}^{sk}$, e $\forall x_1 \ldots x_n y(\varphi(x_1, \ldots, x_n, y) \leftrightarrow y = f_\varphi(x_1, \ldots, x_n))$ é chamada de *definição* de $F_\varphi$ em $\mathrm{A}^{sk}$.

Podemos de bom senso esperar que com respeito às funções de Skolem a combinação $\forall\exists!$ conduz a melhores resultados que a combinação $\forall\exists$. O teorema seguinte nos diz que obtemos substancialmente mais que apenas um resultado de extensão conservativa.

**Teorema 3.4.6** *Suponha que $T \vdash \forall x_1 \ldots x_n \exists! y \varphi(x_1, \ldots, x_n, y)$, onde $VL(\varphi) = \{x_1, \ldots, x_n, y\}$ e seja $f$ um símbolo n-ário que não ocorre em $T$ ou em $\varphi$. Então $T^+ = T \cup \{\forall x_1 \ldots x_n y(\varphi(x_1, \ldots, x_n, y) \leftrightarrow y = f(x_1, \ldots, x_n))\}$ é conservativa sobre $T$.*
*Além do mais, existe uma tradução $\tau \rightarrow \tau^0$ de $L^+ = L \cup \{f\}$ para $L$, tal que*

(1) $T^+ \vdash \tau \leftrightarrow \tau^0$,
(2) $T^+ \vdash \tau \Leftrightarrow T \vdash \tau^0$,
(3) $\tau = \tau^0$ *para* $\tau \in L$.

*Demonstração.* Semelhante à demonstração acima, porém mais simples. Indicamos os passos; os detalhes deixo ao leitor.

(a) Seja A do tipo de $L$. Expanda A para $\mathrm{A}^+$ pela adição de uma relação $Q^+ = \{\langle a_1, \ldots, a_n \rangle \mid \mathrm{A} \models \varphi(\overline{a}_1, \ldots, \overline{a}_n)\}$.

(b) Mostre que $\mathrm{A} \models T \Leftrightarrow \mathrm{A}^+ \models T^+$ e conclua (i).

(c) Imite a tradução definida no teorema 3.4.6.

$\square$

Chamamos as extensões mostradas em 3.4.6, 3.4.7 e 3.4.8, de *extensões por definição*. As sentenças
$\forall x_1 \ldots x_n y(\varphi \leftrightarrow y = f(x_1, \ldots, x_n))$,
$\forall x_1 \ldots x_n(f(x_1, \ldots, x_n = t)$,
$\forall x_1 \ldots x_n(\varphi \leftrightarrow Q(x_1, \ldots, x_n))$,
são chamadas *axiomas definidores* para $f$ e $Q$ respectivamente.

A Extensão por Definição faz parte da prática diária da matemática (e da ciência em geral). Se uma certa noção, definível em uma dada linguagem, tem um papel importante em nossas considerações, então é conveniente se ter uma notação curta, fácil, para tal noção.

Pense em "$x$ é um n'umero primo", "$x$ é igual a $y$ ou menor que $y$", "$x$ é o máximo de $x$ e $y$", etc.

*Exemplos.*
1. *Funções características*

Considere uma teoria $T$ com (no mínimo) duas constantes $c_0, c_1$, tal que $T \vdash c_0 \neq c_1$. Seja $VL(\varphi) = \{x_1, \ldots, x_n\}$, então $T \vdash \forall x_1 \ldots x_n \exists! y(\varphi \wedge y = c_1) \vee (\neg\varphi \wedge y = c_0))$. (Mostre isso diretamente ou use o Teorema da Completude.)

O axioma definidor para a função característica $K_\varphi$ é
$\forall x_1 \ldots x_n y((\varphi \wedge y = c_0) \vee (\neg\varphi \wedge y = c_1)) \leftrightarrow y = K_\varphi(x_1, \ldots, x_n))$.

2. *Definições por Recursão (Primitiva)*

Em aritmética frequentemente se introduz funções por recursão, e.g. $x!$, $x^y$. O estudo dessas funções e similares pertence à teoria da recursão; aqui apenas chamamos a atenção para o fato de que podemos adicionar conservativamente símbolos e axiomas para tais funções. *Fato* (Gödel, Davis, Matijasevich): cada função recursiva é definível em **PA**, no sentido de que existe uma fórmula $\varphi$ de **PA** tal que

(i) $\mathbf{PA} \vdash \forall x_1 \ldots x_n \exists! y \varphi(x_1, \ldots, x_n, y)$ e

(ii) para $k_1, \ldots, k_n$, $m \in N$, $f(k_1, \ldots, k_n) = m \Rightarrow \mathbf{PA} \vdash \varphi(\overline{k}_1, \ldots, \overline{k}_n, \overline{m})$.

Para maiores detalhes, ver *Smorynski*, 1991; *Davis*, 1958.

Antes de terminar este capítulo, vamos brevemente retornar ao tópico de funções de Skolem e expansões de Skolem. Como observamos anteriormente, a introdução de funções de Skolem nos permite descartar certos quantificadores existenciais em fórmulas. Exploraremos essa idéia para reescrever fórmulas como fórmulas universais (em uma linguagem estendida!).

Primeiro transformamos a fórmula $\varphi$ na forma normal prenex $\varphi'$. Vamos supor que $\varphi' = \forall x_1 \ldots x_n \exists y \psi(x_1, \ldots, x_n, y, z_1, \ldots, z_k)$, onde $z_1, \ldots, z_k$ são todas as variáveis livres em $\varphi$. Agora considere

$$T^* = T \cup \{\forall x_1 \ldots x_n z_1 \ldots z_k(\exists y \psi(x_1, \ldots, x_n, y, z_1, \ldots, z_k) \rightarrow \psi(x_1, \ldots, x_n, f(x_1, \ldots, x_n, z_1, \ldots, z_k), z_1, \ldots, z_k))\}.$$

Pelo Teorema 3.4.4 $T^*$ é conservativa sobre $T$, e é um exercício simples em lógica mostrar que
$T^* \vdash \forall x_1 \ldots x_n \exists y \psi(-, y, -) \leftrightarrow \forall x_1 \ldots x_n \psi(-, f(\ldots), -)$.

Agora repetimos o processo e eliminamos o próximo quantificador existencial no prefixo de $\psi$; em um número finito de passos obtemos uma fórmula $\varphi^*$ em forma normal prenex sem quantificadores existenciais, que, em uma extensão conservativa apropriada de $T$ obtida por uma série de expansões de Skolem, é equivalente a $\varphi$.

**Advertência:** A *forma de Skolem* $\varphi^*$ é um tipo diferente de forma normal, no sentido de que ela não é *logicamente equivalente* a $\varphi$.

O Teorema 3.4.4 mostra que a adição de Axiomas de Skolem a uma teoria é conservativa, de modo que podemos operar com segurança com formas de Skolem. A forma de Skolem $\varphi^*$ tem a propriedade de que é satisfatível se e somente se $\varphi$ também o é (cf. Exercício 4). Por conseguinte ela é às vezes chamada a forma de Skolem para satisfatibilidade. Existe uma forma dual de Skolem $\varphi_s$ (cf. Exercício 5), que é válida se e somente se $\varphi$ também o é. $\varphi_s$ é chamada a forma de Skolem para validade.

*Exemplo.* $\forall x_1 \exists y_1 \exists y_2 \forall x_2 \exists y_3 \forall x_3 \forall x_4 \exists y_4\, \varphi(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4, z_1, z_2)$.

passo 1. Eliminar $y_1$:

$$\forall x_1 \exists y_2 \forall x_2 \exists y_3 \forall x_3 \forall x_4 \exists y_4\, \varphi(x_1, x_2, x_3, x_4, f(x_1, z_1, z_2), y_2, y_3, y_4, z_1, z_2).$$

passo 2. Eliminar $y_2$:

$$\forall x_1 \forall x_2 \exists y_3 \forall x_3 \forall x_4 \exists y_4\, \varphi(\ldots, f(x_1, z_1, z_2), g(x_1, z_1, z_2), y_3, y_4, z_1, z_2).$$

passo 3. Eliminar $y_3$:

$$\forall x_1 \forall x_2 \forall x_3 \forall x_4 \exists y_4\, \varphi(\ldots, f(x_1, z_1, z_2), g(x_1, z_1, z_2), h(x_1, x_2, z_1, z_2), y_4, z_1, z_2).$$

passo 4. Eliminar $y_4$:

$$\forall x_1 \forall x_2 \forall x_3 \forall x_4\, \varphi(\ldots, f(x_1, z_1, z_2), g(x_1, z_1, z_2), h(x_1, x_2, z_1, z_2), k(x_1, x_2, x_3, x_4, z_1, z_2), z_1, z_2).$$

Em expansões de Skolem temos funções disponíveis que pegam elementos para nós. Podemos explorar isso para obter extensões elementares.

**Teorema 3.4.7** *Considere* $\mathrm{A}$ *e* $\mathrm{B}$ *do mesmo tipo. Se* $\mathrm{B}^{sk}$ *é uma expansão de Skolem de* $\mathrm{B}$ *e* $\mathrm{A}^* \subseteq \mathrm{B}^{sk}$*, onde* $\mathrm{A}^*$ *é alguma expansão de* $\mathrm{A}$*, então* $\mathrm{A} \prec \mathrm{B}$*.*

*Demonstração.* Usamos o Exercício 7 da seção 3.3. Sejam $a_1, \ldots, a_n \in |\mathrm{A}|$, $\mathrm{B} \models \exists y \varphi(y, \overline{a}_1, \ldots, \overline{a}_n) \Leftrightarrow \mathrm{B}^{sk} \models \varphi(f_\varphi(\overline{a}_1, \ldots, \overline{a}_n), \overline{a}_1, \ldots, \overline{a}_n)$, onde $f_\varphi$ é a função de Skolem para $\varphi$. Como $\mathrm{A}^* \subseteq \mathrm{B}^{sk}$, $f_\varphi^{\mathrm{A}^*}(a_1, \ldots, a_n) = f_\varphi^{\mathrm{B}^{sk}}(a_1, \ldots, a_n)$ e portanto $b = (f_\varphi(\overline{a}_1, \ldots, \overline{a}_n))^{\mathrm{B}^{sk}} = (f_\varphi(\overline{a}_1, \ldots, \overline{a}_n))^{\mathrm{A}^*} \in |\mathrm{A}|$. Daí $\mathrm{B}^{sk} \models \varphi(\overline{b}, \overline{a}_1, \ldots, \overline{a}_n)$. Isso mostra que $\mathrm{A} \prec \mathrm{B}$. $\square$

**Definição 3.4.8** Seja $X \subseteq |\mathrm{A}|$. A *Envoltória de Skolem* $\mathrm{S}_X$ de $X$ é a subestrutura de $\mathrm{A}$ que é o reduto da estrutura gerada por $X$ na expansão de Skolem $\mathrm{A}^{sk}$ de $\mathrm{A}$ (cf. Exercício 14, seção 3.3).

Em outras palavras $\mathrm{S}_X$ é a menor subestrutura de $\mathrm{A}$, contendo $X$, que é fechada sob todas as funções de Skolem (incluindo as constantes).

**Corolário 3.4.9** *Para todo* $X \subseteq |\mathrm{A}|$*,* $\mathrm{S}_X \prec \mathrm{A}$*.*

Agora obtemos imediatamente a versão mais forte do Teorema de Skolem–Löwenheim de-cima-para-baixo formulada no Teorema 3.3.12, observando que a cardinalidade de uma subestrutura gerada por $X$ é a maior entre as cardinalidades de $X$ e a da linguagem. Isso se verifica também no caso em questão, onde um número infinito de funções de Skolem são adicionadas à linguagem).

**Exercícios**

1. Considere o exemplo sobre a função característica.

   (i) Mostre que $T^+ \vdash \forall x_1 \ldots x_n(\varphi \leftrightarrow K_\varphi(x_1, \ldots, x_n) = c_1)$.

   (ii) Traduza $K_\varphi(x_1, \ldots, x_n) = K_\varphi(y_1, \ldots, y_n)$.

   (iii) Mostre que $T^+ \vdash \forall x_1 \ldots x_n y_1 \ldots y_n(K_\varphi(x_1, \ldots, x_n) = K_\varphi(y_1, \ldots, y_n)) \leftrightarrow \forall x_1 \ldots x_n \varphi(x_1, \ldots, x_n) \vee \forall x_1 \ldots x_n \neg\varphi(x_1, \ldots, x_n)$.

2. Determine as formas de Skolem de

   (a) $\forall y \exists x(2x^2 + yx - 1 = 0)$,

   (b) $\forall \varepsilon \exists \delta(\varepsilon > 0 \to (\delta > 0 \wedge \forall x(|x - \overline{a}| < \delta \to |f(x) - f(\overline{a})| < \varepsilon)$,

   (c) $\forall x \exists y(x = f(y))$,

   (d) $\forall xy(x < y \to existsu(u < x) \wedge \exists v(y < v) \wedge \exists w(x < v \wedge w < y))$,

   (e) $\forall x \exists y(x = y^2 \vee x = -y^2)$.

3. Seja $\sigma^s$ a forma de Skolem de $\sigma$. Considere apenas sentenças.

   (i) Mostre que $\Gamma \cup \{\sigma^*\}$ é conservativa sobre $\Gamma \cup \{\sigma\}$.

   (ii) Faça $\Gamma^s = \{\sigma^s \mid \sigma \in \Gamma\}$. Mostre que para $\Gamma$ finita, $\Gamma^s$ é conservativa sobre $\Gamma$.

   (iii) Mostre que $\Gamma^s$ é conservativa sobre $\Gamma$ para $\Gamma$ arbitrária.

4. Uma fórmula $\varphi$ com $VL(\varphi) = \{x_1, \ldots, x_n\}$ é chamada de *satisfatível* se existe uma A e $a_1, \ldots, a_n \in |A|$ tal que $A \models \varphi(\overline{a}_1, \ldots, \overline{a}_n)$. Mostre que $\varphi$ é satisfatível sse $\varphi^s$ é satisfatível.

5. Consideramos uma linguagem $L$ com pelo menos um símbolo de constante. Seja $\sigma$ uma sentença em forma normal prenex. Definimos a *forma dual de Skolem* $\sigma_s$ de $\sigma$ da seguinte maneira: seja $\sigma = (Q_1 x_1) \ldots (Q_n x_n)\tau$, onde $\tau$ é livre de quantificador e os $Q_i$'s são quantificadores. Considere $\sigma' = (\overline{Q}_1 x_1) \ldots (\overline{Q}_n x_n)\neg\tau$, onde $\overline{Q}_i = \forall, \exists$ sse $Q_i = \exists, forall$. Suponha que $(\sigma')^s = (\overline{Q}_{i_1} x_{i_1}) \ldots (\overline{Q}_{i_k} x_{i_k} \neg\tau'$; então $\sigma_s = (Q_{i_1} x_{i_1}) \ldots (Q_{i_k} x_{i_k})\tau'$.

   Em palavras: elimine de $\sigma$ os quantificadores universais e suas variáveis tal qual os existenciais no caso da forma de Skolem. Findamos com uma sentença universal.

   *Exemplo.* $(\forall x \exists y \forall z \varphi(x, y, z))_s = \exists y \varphi(c, y, f(y))$.

   (a) Mostre que para todas as sentenças (prenex) $\sigma$, $\models \sigma$ sse $\models \sigma_s$. (Sugestão: veja o Exercício 4). Daí o nome "forma de Skolem para *validade*".

   (b) Demonstre o *Teorema de Herbrand*

   $$\vdash \sigma \quad \Leftrightarrow \quad \bigvee_{i=1}^{m} \sigma'_s(t_1^i, \ldots, t_n^i)$$

   para algum $m$, onde $\sigma'_s$ é obtida de $\sigma_s$ removendo os quantificadores. Os $t_j^i$ $(i \leq m, j \leq n)$ são certos termos fechados na expansão dual de Skolem de $L$. Sugestão: olhe para $\neg(\neg\sigma)^s$. Use o Exercício 18, seção 3.3.

6. Suponha que $T \vdash \exists x \varphi(x)$, com $VL(\varphi) = \{x\}$. Mostre que qualquer modelo A de $T$ pode ser expandido para um modelo $\mathrm{A}^*$ de $T$ com uma constante adicional $c$ tal que $\mathrm{A}^* \models \varphi(c)$. Use isso para construir uma demonstração alternativa de 3.4.1.

7. Considere $I_\infty$ a teoria da identidade "com universo infinito" com axiomas $\lambda_n$ $(n \in N)$ e $I'_\infty$ com constantes adicionais $c_i$ $(i \in N)$ e axiomas $c_i \neq c_j$ para $i \neq j$, $i, j \in N$. Mostre que $I'_\infty$ é conservativa sobre $I_\infty$.