Chapter 2

A Lógica de Primeira Ordem

Nesta seção vamos em um certo sentido estender a Lógica Proposicional para ganhar em poder de expressividade. Como é a gramática da Lógica de Primeira Ordem (LPO)? Isto é, qual a linguagem que precisamos para conseguir expressar quantificação universal e existencial? Inicialmente, precisamos representar os elementos que podem ser quantificados. Assim, diferentemente do caso proposicional, temos duas classes de objetos na LPO: *termos* e *fórmulas*. Os termos são representados pela seguinte gramática:

$$t ::= x \mid f(t, \ldots, t) \tag{2.1}$$

ou seja, os termos são construídos a partir de variáveis (no sentido usual da palavra em Matemática) e, funções com uma certa aridade (i.e número de argumentos). Observe que os termos vão representar os elementos do conjunto sobre o qual podemos quantificar e caracterizar por meio de propriedades. Por exemplo, considere o conjunto dos números naturais $\mathbb{N}$. Neste caso, as variáveis representam números naturais, e exemplos de funções são: sucessor (aridade 1), soma (aridade 2), etc. O conjunto das variáveis de um termo t, notação (t), consiste no conjunto das variáveis que ocorrem em t, e pode ser definido indutivamente por:

Definição 62. *O conjunto $var(t)$ das variáveis que ocorrem no termo t é definido indutivamente como a seguir:*

1. $var(x) = \{x\}$;

2. $var(f(t_1, t_2, \ldots, t_n)) = var(t_1) \cup var(t_2) \cup \ldots \cup var(t_n)$.

Denotaremos por $t[[x/u]]$ o termo obtido ao se substituir todas as ocorrências da variável x pelo termo u no termo t.

As fórmulas da LPO utilizam os mesmos conectivos da LP e são definidas pela seguinte gramática:

$$\varphi ::= p(t, \ldots, t) \mid \bot \mid (\neg\varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \to \varphi) \mid \exists_x \varphi \mid \forall_x \varphi \tag{2.2}$$

onde o primeiro construtor representa uma fórmula atômica, e os dois últimos representam, respectivamente, a quantificação existencial e universal. Note que as fórmulas atômicas representam fórmulas que não podem ser decompostas, e que têm termos como argumentos. Em uma fórmula atômica da forma $p(t_1, \ldots, t_n)$, p é um *predicado* de aridade n, e $t_1, \ldots, t_n$ são termos. A LPO é a lógica utilizada no dia a dia dos matemáticos, ainda que de maneira informal. Com os predicados podemos expressar propriedades dos termos. Por exemplo, ainda no conjunto dos números naturais, podemos expressar a propriedade de um número natural ser primo por meio de um predicado unário, digamos p. Desta forma, a fórmula $p(x)$ pode expressar o fato de x ser primo. Outros exemplos de fórmulas atômicas incluem os predicados $\leq$,

$\geq$, $<$ e $>$ que normalmente usamos em notação infixa como em $2 \leq 5$, por exemplo.

Observe que agora existem dois tipos de variáveis na linguagem da Lógica de Primeira Ordem. Por exemplo, considere as fórmulas $q(x)$ e $\forall_x p(x)$. Em $\forall_x p(x)$ ocorrência da variável x em $p(x)$ está **ligada** ao quantificador universal, enquanto que na fórmula $q(x)$, a variável x está **livre**. De uma forma geral, dizemos que uma ocorrência de uma variável é ligada, se ela estiver no escopo de um quantificador (universal ou existencial), e livre, se a ocorrência não estiver no escopo de nenhum quantificador. Observe que uma variável pode ocorrer livre e ligada em uma mesma fórmula: $q(x) \vee \forall_x p(x)$. O conjunto das variáveis livres de uma fórmula φ, notação $FV(\varphi)$, é definido indutivamente como segue:

Definição 63. *Seja φ uma fórmula da Lógica de Primeira Ordem. O conjunto $FV(\varphi)$ das variáveis livres da fórmula φ é definido indutivamente na estrutura de φ por:*

1. $FV(p(t_1, t_2, \ldots, t_n)) = var(t_1) \cup var(t_2) \cup \ldots \cup var(t_n)$;
2. $FV(\bot) = \{\}$;
3. $FV(\neg\psi) = FV(\psi)$;
4. $FV(\psi \star \gamma) = FV(\psi) \cup FV(\gamma)$, *onde* $\star \in \{\wedge, \vee, \rightarrow\}$;
5. $FV(Q_x\psi) = FV(\psi)\backslash\{x\}$, *onde* $Q \in \{\forall, \exists\}$.

De maneira análoga podemos definir o conjunto das variáveis ligadas de uma fórmula:

Definição 64. *Seja φ uma fórmula da Lógica de Primeira Ordem. O conjunto $BV(\varphi)$ das variáveis ligadas da fórmula φ é definido indutivamente na estrutura de φ por:*

1. $BV(p(t_1, t_2, \ldots, t_n)) = \{\}$;
2. $BV(\bot) = \{\}$;
3. $BV(\neg\psi) = BV(\psi)$;
4. $BV(\psi \star \gamma) = BV(\psi) \cup BV(\gamma)$, *onde* $\star \in \{\wedge, \vee, \rightarrow\}$;
5. $BV(Q_x\psi) = BV(\psi) \cup \{x\}$, *onde* $Q \in \{\forall, \exists\}$.

Estas noções são importantes porque a operação de substituição na Lógica de Primeira Ordem é definida de tal forma a evitar captura de variáveis, diferentemente da substituição feita em termos vista anteriormente. Isto significa que, por exemplo, se quisermos substituir a ocorrência de y em $\forall_x p(x, y)$ por x, o resultado não pode ser $\forall_x p(x, x)$ já que neste caso a segunda ocorrência de x que era livre, passou a ser ligada depois da substituição, ou seja, a segunda ocorrência de x foi capturada. Para evitar este problema, podemos renomear as variáveis ligadas de uma fórmula sempre que necessário. De fato, observe que as fórmulas $\forall_x q(x)$, $\forall_y q(y)$ e $\forall_z q(z)$ têm todas a mesma semântica. Isto significa que o renomeamento de variáveis ligadas não muda o sentido, ou significado, de uma fórmula. Para

enfatizarmos a operação de substituição que definiremos a seguir, denotaremos por $\varphi[x/t]$ o resultado de substituir todas as ocorrências livres de x na fórmula φ pelo termo t. Quando a variável a ser substituída não precisar ser enfatizada (por exemplo, por poder ser facilmente obtida do contexto), escreveremos simplesmente $\varphi(t)$ ao invés de $\varphi[x/t]$.

Definição 65. *Seja φ uma fórmula da Lógica de Primeira Ordem. A operação de substituir todas as ocorrências livres da variável x pelo termo t em φ, notação $\varphi[x/t]$ é definida indutivamente na estrutura da fórmula φ da seguinte forma:*

1. $p(t_1, t_2, \ldots, t_n)[x/t] = p(t_1[[x/t]], t_2[[x/t]], \ldots, t_n[[x/t]])$;

2. $\bot[x/t] = \bot$;

3. $(\neg\psi)[x/t] = \neg(\psi[x/t])$;

4. $(\psi \star \gamma)[x/t] = (\psi[x/t]) \star (\gamma[x/t])$, *onde* $\star \in \{\vee, \wedge, \rightarrow\}$;

5. $(Q_y\psi)[x/t] = \begin{cases} Q_y\psi, & \text{se } x = y; \\ Q_y(\psi[x/t]), & \text{se } y \notin var(t); \\ Q_z(\psi[y/z][x/t]), & \text{c.c.} \end{cases}$
   onde z é uma variável nova, e $Q \in \{\forall, \exists\}$.

Observe que o primeiro caso do item 5 da definição anterior, a substituição não tem nenhum efeito sobre a fórmula quando a variável da substituição coincide com a variável do quantificador ($x = y$), e portanto variáveis ligadas não são substituídas. O caso em que $y \notin var(t)$ faz a propagação da substituição para dentro do corpo do quantificador já que não há possibilidade de captura de variável. Por fim, quando $x \neq y$ e $y \in var(t)$ a variável do quantificador é renomeada para um nome novo, no caso z, as ocorrências de y em ψ são renomeadas para z e então a substituição é propagada para dentro do corpo do quantificador.

O sistema de dedução natural na LPO possui as mesmas regras utilizadas no caso proposicional, mas agora aplicadas a fórmulas da LPO, e adicionalmente temos as regras de introdução e eliminação para os quantificadores que apresentamos a seguir.

A regra de introdução do quantificador universal permite a construção de uma prova de uma fórmula da forma $\forall_x\varphi(x)$, ou seja, queremos concluir que a propriedade φ é satisfeita por qualquer elemento x do domínio. Mas o que precisamos para garantir que todo elemento x do domínio tenha a propriedade φ? Uma maneira seria tentar a construção individual de cada uma destas provas, ou seja, suponha que o domínio seja o conjunto $\{x_0, x_1, x_2 \ldots\}$ que pode ser finito ou infinito, e considere uma prova de $\varphi(x_0)$, isto é, uma prova de que x_0 satisfaz a propriedade φ. Seria possível repetir esta prova para x_1, x_2, e assim sucessivamente? Se pudermos repetir a mesma prova para todos os elementos do domínio então certamente podemos concluir $\forall_x\varphi(x)$. Para que uma generalização desta forma seja possível precisamos que a prova de $\varphi(x_0)$ não dependa de hipótese que assuma alguma informação sobre x_0.

$$\frac{\varphi(x_0)}{\forall_x\varphi(x)}\ (\forall_i)$$ se a prova de $\varphi(x_0)$ não depende de hipótese não-descartada que contenha x_0.

A regra de eliminação do quantificador universal nos permite instanciar a variável quantificada universalmente x com qualquer elemento t do domínio.

$$\frac{\forall_x \varphi(x)}{\varphi(t)}\ (\forall_e)$$

A analogamente, a regra de introdução do quantificador existencial nos permite concluir que existe um elemento que satisfaz a propriedade φ a partir da prova de que algum elemento do domínio, digamos t, satisfaça a propriedade φ.

$$\frac{\varphi(t)}{\exists_x \varphi(x)}\ (\exists_i)$$

Por fim, a regra de eliminação do quantificador existencial é dada como a seguir:

$$\frac{\exists_x \varphi(x) \qquad \begin{array}{c}[\varphi(x_0)]^u \\ \vdots \\ \gamma\end{array}}{\gamma}\ (\exists_e)\ u$$

onde x_0 é uma variável nova que não ocorre em γ.

Nesta regra provamos γ a partir de uma prova de $\exists_x \varphi(x)$, e de uma prova de γ a partir da suposição $\varphi(x_0)$. Ou seja, como temos uma prova de $\exists_x \varphi(x)$, então temporariamente assumimos que x_0 (um novo elemento que, portanto, não pode ter sido utilizado antes) satisfaz a propriedade φ. Se a partir desta suposição pudermos provar uma fórmula, digamos γ, que não dependa de x_0 então podemos concluir γ após descartar a suposição $\varphi(x_0)$.

Exercício 66. *Apresente derivações em Dedução Natural para os sequentes $\forall_x \neg\varphi \dashv\vdash \neg\exists_x \varphi$ na lógica minimal.*

Exercício 67. *Apresente derivações em Dedução Natural para os sequentes $\neg\forall x\, \phi \dashv\vdash \exists x\, \neg\phi$, em seguida classifique cada prova como minimal, intuicionista ou clássica.*

Exercício 68. *Apresente derivações em Dedução Natural para os sequentes $\forall x\, \phi \dashv\vdash \neg\exists x\, \neg\phi$, em seguida classifique cada prova como minimal, intuicionista ou clássica.*

Exercício 69. *Apresente derivações em Dedução Natural para os sequentes $\exists x\, \phi \dashv\vdash \neg\forall x\, \neg\phi$, em seguida classifique cada prova como minimal, intuicionista ou clássica.*

Exercício 70. *Apresente derivações em Dedução Natural para os sequentes a seguir assumindo que x não ocorre livre em ψ, em seguida classifique cada prova como minimal, intuicionista ou clássica.*

1. $(\forall x\, \phi) \wedge \psi \vdash \forall x\, (\phi \wedge \psi)$
2. $(\exists x\, \phi) \wedge \psi \vdash \exists x\, (\phi \wedge \psi)$
3. $\forall x\, (\psi \to \phi) \vdash \psi \to \forall x\, \phi$
4. $\forall x\, (\phi \to \psi) \vdash (\exists x\, \phi) \to \psi$

Exercício 71. *Prove que não existe uma derivação intuicionista para os sequentes a seguir:*

1. $\neg\exists_x\neg\varphi \vdash \forall_x\varphi$

2. $\neg\forall_x\neg\varphi \vdash \exists_x\varphi$

3. $\varphi \to \psi \vdash (\neg\varphi) \vee \psi$

Assim como a lógica proposicional, a lógica de primeira ordem é correta e completa, mas estes resultados não serão provados aqui (Veja [4]).

2.1 Indução

Indução é uma técnica de prova muito poderosa que desempenha um papel fundamental tanto em Matemática quanto em Computação. Estudaremos esta técnica no contexto dos conjuntos definidos indutivamente, mas o leitor interessado em se aprofundar no tema pode pesquisar sobre *indução transfinita* [15](?? jech). Um conjunto, digamos, A, é *definido indutivamente* se seus elementos podem ser construídos a partir de um conjunto finito de regras de inferência da forma de um axioma:

$$\frac{}{a \in A}$$

ou seja, este axioma diz que a é um elemento do conjunto A. Ou então, os elementos podem ser definidos a partir de uma regra de inferência indutiva:

$$\frac{a_1 \in A \qquad a_2 \in A \ldots\ a_n \in A}{a \in A}$$

Neste caso, temos que se $a_1, a_2, \ldots, a_n$ são elementos de A então a também é um elemento de A. Por exemplo, qualquer conjunto finito pode ser definido indutivamente com um axioma para cada elemento. De fato, o conjunto Sem dos dias da semana pode ser definido indutivamente via 7 axiomas:

$$\frac{}{\text{domingo} \in Sem}\ (\textsc{dom}) \qquad \frac{}{\text{segunda-feira} \in Sem}\ (\textsc{seg}) \qquad \frac{}{\text{terça-feira} \in Sem}\ (\textsc{ter})$$

$$\frac{}{\text{quarta-feira} \in Sem}\ (\textsc{qua}) \qquad \frac{}{\text{quinta-feira} \in Sem}\ (\textsc{qui}) \qquad \frac{}{\text{sexta-feira} \in Sem}\ (\textsc{sex})$$

$$\frac{}{\text{sábado} \in Sem}\ (\textsc{sab})$$

Alternativamente, podemos utilizar uma notação mais compacta definir o conjunto Sem: se d é uma variável que representa um elemento qualquer de Sem então a gramática a seguir é equivalente à definição via as 7 regras de inferência apresentadas acima:

$$d ::= \text{domingo} \mid \text{segunda-feira} \mid \text{terça-feira} \mid \text{quarta-feira} \mid \text{quinta-feira} \mid \text{sexta-feira} \mid \text{sábado}$$

Mas conjuntos definidos indutivamente também podem ser infinitos. O exemplo mais conhecido provavelmente é o conjunto dos números naturais $\mathbb{N}$, que pode ser definido pelas regras de inferência a seguir:

$$\frac{}{0 \in \mathbb{N}} \qquad \frac{n \in \mathbb{N}}{S\ n \in \mathbb{N}}$$

Neste caso, a regra da esquerda é um axioma que diz que o 0 é um número natural, enquanto que a regra da direita diz que se n é um número natural então $S\ n$ (o sucessor de n) também é um número natural. A gramática equivalente a estas duas regras é dada por:

$$n ::= 0 \mid S\ n \tag{2.3}$$

Agora que sabemos o que são conjuntos definidos indutivamente podemos voltar ao tema da indução, que é uma técnica de prova que nos permite provar propriedades de conjuntos definidos indutivamente. Como provar que os elementos de um conjunto definido indutivamente, digamos A, satisfazem uma dada propriedade P? Se o conjunto A for finito então podemos testar individualmente se cada elemento satisfaz a propriedade P. Mesmo que A seja um conjunto grande, depois de uma quantidade finita de tempo teremos uma prova de que os elementos de A satisfazem a propriedade P. E se o conjunto A for infinito? A ideia é bastante intuitiva: suponha que os elementos deste conjunto possam ser colocados um após o outro como peças de um dominó, de tal forma que, se uma peça qualquer for derrubada então a peça que está logo em seguida também é derrubada. Então podemos concluir, que se a primeira peça for derrubada então **todas** as outras serão derrubadas. Ou seja, voltando ao contexto de propriedades de elementos de um conjunto, a ideia é provar que se um elemento arbitrário do conjunto satisfaz a propriedade então o próximo elemento também satisfaz a propriedade. Se esta prova puder ser feita juntamente com a prova de que o primeiro elemento do conjunto também satisfaz a propriedade então podemos concluir que todos os elementos do conjunto satisfazem a propriedade.

Vamos iniciar este estudo sobre indução no contexto dos números naturais, onde esta noção de ordem é bem clara: o primeiro elemento é o 0, em seguida vem o 1, depois o 2, etc. De uma forma geral, depois de um número natural k vem o natural $S\ k$, o sucessor de k que também escrevemos como $k + 1$. A indução no contexto dos números naturais é conhecida como *indução matemática*, e será explorada na próxima seção.

A gramática (2.3) possui dois construtores: 0 e S. O primeiro diz que 0 é um número natural, e o segundo diz que a partir de um natural já construído, digamos n, podemos construir um outro natural, a saber, $S\ n$, ou seja, o sucessor de n. Muito bem, agora considere uma propriedade qualquer dos números naturais. Por exemplo, a que diz que a soma dos n primeiros números ímpares é igual a n^2. Como podemos provar esta propriedade? Isto mesmo, por indução! O que diz mesmo o princípio de indução para os números naturais? Diz que se uma propriedade P vale para 0 (base da indução), e se, supondo que P vale para um natural arbitrário k (hipótese de indução), podemos provar que ela vale também para $S\ k$ (o sucessor de k)[1] (passo indutivo) então podemos concluir que P vale para todos

[1] Note que o sucessor de k pode ser escrito como $S\ k$ ou $k + 1$.

os números naturais. Esquematicamente, podemos apresentar este princípio, denominado *Princípio da Indução Matemática (PIM)*, como a seguir:

$$\frac{P\ 0 \qquad \forall k, P\ k \Longrightarrow P\ (S\ k)}{\forall n, P\ n}\ (PIM)$$

Exemplo 72. *Queremos provar que a soma dos n primeiros números ímpares é igual a n^2. Esta propriedade vale trivialmente para o 0 (a soma dos 0 primeiros números ímpares é igual a 0^2). Agora suponha que a soma dos k primeiros números ímpares seja igual a k^2 (hipótese de indução). O $(k+1)$-ésimo número ímpar é igual a $2.k+1$ (por que?), e portanto a soma dos $k+1$ primeiros números ímpares é $k^2+2.k+1=(k+1)^2$, como queríamos provar.*

Uma outra forma de resolver este problema em um contexto mais formal pode ser feita a partir de uma definição formal da soma dos n primeiros números ímpares por meio do somatório $\sum_{i=1}^{n}(2.i-1)$, que por definição é igual a 0, se $n=0$. Queremos provar que $\sum_{i=1}^{n}(2.i-1)=n^2$, para todo número natural n. Aplicando o princípio da indução, teremos 2 casos para analisar:

- *(**Base da indução**): A base da indução se dá quando $n=0$, e é trivial porque o lado esquerdo da igualdade é igual a 0 por definição.*

- *(**Passo indutivo**): O passo indutivo é a parte interessante de qualquer prova por indução. Neste caso específico, vamos assumir que a propriedade que queremos provar vale para um número natural arbitrário, digamos k, e provaremos que esta propriedade continua valendo para o natural $k+1$. Ou seja, assumimos que $\sum_{i=1}^{k}(2.i-1)=k^2$, e vamos provar que $\sum_{i=1}^{k+1}(2.i-1)=(k+1)^2$. Partindo do lado esquerdo desta igualdade, podemos decompor o somatório da seguinte forma $\sum_{i=1}^{k+1}(2.i-1)=\sum_{i=1}^{k}(2.i-1)+(2.k+1)$, e agora podemos utilizar a hipótese de indução (h.i.) para assim chegarmos ao lado direito da igualdade: $\sum_{i=1}^{k+1}(2.i-1)=\sum_{i=1}^{k}(2.i-1)+(2.k+1)\overset{h.i.}{=}k^2+(2.k+1)=(k+1)^2$.*

Por fim, apresentamos esta prova na forma de árvore:

$$\dfrac{\dfrac{0=0}{\sum_{i=1}^{0}(2.i-1)=0^2} \qquad \dfrac{\dfrac{\dfrac{[\sum_{i=1}^{k}(2.i-1)=k^2]^u}{\sum_{i=1}^{k}(2.i-1)+(2.k+1)=(k+1)^2}}{\sum_{i=1}^{k+1}(2.i-1)=(k+1)^2}(\rightarrow_i)\ u}{\sum_{i=1}^{k}(2.i-1)=k^2 \rightarrow \sum_{i=1}^{k+1}(2.i-1)=(k+1)^2}}{\sum_{i=1}^{n}(2.i-1)=n^2}\ (\text{Ind. em } n)$$

Exercício 73. *Prove que a soma dos n primeiros números naturais é igual a $\frac{n(n+1)}{2}$. Ou seja, mostre que $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.*

Exercício 74. *Prove que a soma dos n primeiros quadrados é igual a* $\frac{n(n+1)(2n+1)}{6}$*. Ou seja, mostre que* $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

Exercício 75. *Prove que* $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.

Exercício 76. *Prove que a soma dos n primeiros cubos é igual ao quadrado da soma de 1 até n, ou seja, que* $1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$.

Exercício 77. *Prove que* $3 \mid (2^{2n} - 1)$ *para todo* $n \geq 0$.

Exercício 78. *Prove que* $3^n \geq n^2 + 3$ *para todo* $n \geq 2$.

Exercício 79. *Prove que* $n! \leq n^n$ *para todo* $n \geq 1$.