Notas de aula de *Lógica para Ciência da Computação*

Aula 1 - Definições indutivas e definições recursivas

Renata de Freitas e *Petrucio Viana*
Departamento de Análise, IME–UFF

6 de agosto de 2014

Sumário

1 Conteúdo e objetivos

Nesta aula abordamos os conjuntos indutivos; as definições indutivas; as provas por indução; os conjuntos indutivos com legibilidade única; e as definições recursivas.

Ao estudar esta aula, devemos ser capazes de (1) entender o que é um conjunto indutivo; (2) entender que um mesmo conjunto indutivo pode ser definido por indução de mais de uma maneira; (3) definir conjuntos indutivos de maneira formal, através de um texto que segue um padrão rígido de redação; (4) entender que a cada definição por indução está associada uma maneira de provar propriedades que valem para todos os elementos do conjunto definido; (5) ler provas por indução; (6) elaborar e redigir provas por indução; (7) entender o que é um conjunto indutivo com legibilidade única; (8) elaborar e redigir definições por recursão.

2 A lógica formal e os principais sistemas lógicos

O objetivo geral da *lógica formal* é a mecanização do raciocínio, ou seja,

a "obtenção de informação a partir de informações prévias" por meio de recursos que podem ser implementados em um computador.

Qualquer forma de raciocínio tem, pelo menos, dois aspectos:

– a *representação da informação* em uma linguagem adequada;

– a *aplicação de mecanismos de inferência* à informação representada, para a obtenção da "nova" informação.

Desta forma, todo *sistema lógico* — que é aparato formal para a representação e obtenção da informação — tem, pelo menos duas partes:

– uma *linguagem*, por meio da qual proposições (ou sentenças) de outras linguagens podem ser expressas;

– um *mecanismo de inferência*, por meio do qual argumentações (ou deduções) efetuadas em outras linguagens podem ser checadas e argumentações (ou deduções) do próprio sistema podem ser efetuadas.

Existe uma grande variedade de sistemas lógicos, alguns criados para analisar certos tipos específicos de informação, outros que servem para múltiplos propósitos. Dentre todos, os considerados mais básicos (não no sentido de trivial mas no sentido de fundamental) são, em uma certa ordem de complexidade:

1. a Lógica dos Conectivos (ou Lógica Sentencial, ou Proposicional);
2. a Lógica Equacional;
3. a Lógica dos Quantificadores (ou Lógica de Primeira Ordem);
4. a Lógica Monádica de Segunda Ordem.

Além destes, muitos outros sistemas são considerados menos básicos, como a Lógica Intuicionista, a Lógica Modal, a Lógica Polivalente, etc. Todos estes sistemas são importantes e possuem inúmeras aplicações na Computação, Filosofia, Linguística, Matemática, etc.

Nesta disciplina, vamos estudar apenas os dois sistemas mais básicos e que são considerados como introdutórios a qualquer domínio da lógica formal: a Lógica dos Conectivos, LC, e a Lógica dos Quantificadores, LQ. Para cada um destes sistemas vamos apresentar uma linguagem formal e mecanismos de inferência, bem como mostrar algumas aplicações nas quais LC e LQ desempenham papéis preponderantes.

Em um certo sentido, a mecanização do raciocínio faz parte do escopo da Lógica desde que esta disciplina foi criada por Aristóteles (384 a.C. – 322 a.C.). O que mudou no decorrer do tempo em que esta ciência evoluiu até alcançar a sua forma atual não foi exatamente o seu objeto de estudo, mas, sim, a maneira como este estudo é efetuado. De

fato, a partir do final do século XVIII, estudiosos como G. Boole (1815 – 1864), A. De Morgan (1806 – 1871), C.S. Peirce (1839 – 1914), G. Frege (1848 – 1925), E. Schröder (1841 – 1902), L. Löwenheim (1878 – 1957), B. Russell (1872 – 1970), A.N. Whitehead (1861 – 1947), A. Tarski (1902 –1983) — e muitos outros que seguiram os primeiros passos empreendidos por estes pioneiros — adaptaram as várias ferramentas matemáticas empregadas na definição de conceitos e na justificativa de proposições, de modo a adequá-las para os estudos lógicos, elevando esta disciplina a um patamar de rigor que só encontra equivalentes nas disciplinas matemáticas mais sofisticadas.

É para este mundo de rigor e aplicações que a nossa disciplina serve de introdução e vamos, inicialmente, considerar algumas adaptações na definição de conjuntos e provas por indução — eventualmente já estudadas em outras disciplinas — que serão necessárias para os nosso estudos de Lógica.

Exercício 2.1 Para os que ficaram curiosos sobre as possíveis aplicações e a história da Lógica, sugerimos o texto

> M. da S. Martins. *Lógica: uma abordagem introdutória.* Ciência Moderna, 2012.

que pode ser encontrado nas boas casas do ramo.

3 Conjuntos indutivos

Usualmente, conjuntos são definidos de duas maneiras:

– pela *listagem* (ou uma *indicação da listagem*) dos seus elementos;

– através de uma *propriedade* aplicada a um outro conjunto.

Exemplo 3.1 (a) O conjunto dos números naturais não nulos, $\mathbb{N}^*$, pode ser definido pela seguinte indicação da listagem dos seus elementos:

$$\mathbb{N}^* = \{1, 2, 3, \ldots, n, \ldots\}$$

(b) Já o conjunto dos números pares não nulos, $\mathbb{P}^*$, pode ser definido pela seguinte indicação da listagem dos seus elementos:

$$\mathbb{P}^* = \{2, 4, 6, \ldots, 2n, \ldots\}$$

(c) Considerando $\mathbb{N}^*$ como dado, $\mathbb{P}^*$ também pode ser definido por uma propriedade:

$$\mathbb{P}^* = \{x \in \mathbb{N}^* : x \text{ é par}\}$$

Definições por listagem só são adequadas para conjuntos finitos e, na prática, apenas para conjuntos finitos "pequenos". Definições por propriedades (aplicadas a conjuntos prévios) podem ser usadas para definir qualquer conjunto mas, dependendo da complexidade da propriedade usada na definição, muitas vezes, elas não são fáceis de manusear.

Exercício 3.1 Determine algumas vantagens ou desvantagens em usarmos as definições de conjuntos por listagem e por propriedade em ambientes computacionais.

Mas há, ainda, uma terceira maneira de se definir conjuntos: a *definição por indução*.

Conjuntos definidos por indução.

Dado um conjunto U, considerado como universo, dizemos que um conjunto $C \subseteq U$ é *definido por indução* quando são dados:

1. Um subconjunto $B \subseteq C$, chamado *base*, cujos elementos são considerados como elementos *básicos* de C.

   Dependendo do caso, B pode ser definido por listagem, por propriedade ou, até mesmo, por indução.

2. Um procedimento que pode ser aplicado iteradamente para *construir* todos os elementos de C a partir dos elementos básicos.

   A descrição deste procedimento pode se dar de diversas formas, dependendo dos pré-requisitos que temos para descrevê-lo.

3. A condição de que nenhum objeto está em C a não ser que possa ser obtido a partir dos elementos básicos por um número finito de aplicações do procedimento de construção descrito.

Exemplo 3.2 (a) O conjunto $\mathbb{N}^* = \{1, 2, 3, \ldots, n, \ldots\}$ dos números naturais não nulos pode ser definido por indução do seguinte modo:

1. Tome o conjunto $\{1\}$, contendo o elemento básico 1, como base.

2. Construa todos os outros elementos de $\mathbb{N}^*$ a partir do 1 por aplicação iterada da operação $n \mapsto n + 1$, de somar uma unidade.

(b) Já o conjunto $\mathbb{P}^* = \{2, 4, 6, \ldots, 2n, \ldots\}$ dos números pares não nulos pode ser definido por indução do seguinte modo:

1. Tome o conjunto $\{2\}$, contendo o elemento básico 2, como base.

2. Construa todos os outros elementos de $\mathbb{P}^*$ a partir do 2 por aplicação iterada da operação $n \mapsto n+2$, de somar duas unidades.

Exercício 3.2 Defina o conjunto $\mathbb{I}^* = \{1, 3, 5, \ldots, 2n+1, \ldots\}$ dos números ímpares não nulos por indução.

Um mesmo conjunto pode ser definido por indução de vários modos, isto é, considerando-se bases diferentes e/ou procedimentos diferentes.

Exemplo 3.3 (a) O conjunto $\mathbb{N}^* = \{1, 2, 3, \ldots, n, \ldots\}$ dos números naturais não nulos também pode ser definido por indução do seguinte modo:

1. Tome o conjunto $\{1, 2, 3, 4, 5\}$, contendo os elementos básicos $1, 2, 3, 4, 5$, como base.
2. Construa todos os outros elementos de $\mathbb{N}^*$ a partir dos números $1, 2, 3, 4, 5$ por aplicação iterada das operações $n \mapsto n+1$, de somar uma unidade, e $n \mapsto n+2$, de somar duas unidades.

(b) O conjunto $\mathbb{N}^* = \{1, 2, 3, \ldots, n, \ldots\}$ dos números naturais não nulos também pode ser definido por indução do seguinte modo, onde Π é o conjunto dos números primos:

1. Tome o conjunto $\Pi \cup \{1\}$, contendo os números primos $2, 3, 5, 7, 11, 13, \ldots$ e a unidade 1, como base.
2. Construa todos os outros elementos de $\mathbb{N}^*$ a partir dos números primos por aplicação iterada da operação $(m, n) \mapsto m \times n$, de multiplicação.

Observe que, no Exemplo 3.3(b), o conjunto base é infinito e foi definido por uma indicação da listagem dos seus elementos.

Exercício 3.3 (i) Defina o conjunto $\Pi = \{2, 3, 5, 7, 11, 13, \ldots\}$ dos números primos por meio de uma propriedade aplicada a $\mathbb{N}^*$.

(ii) Para os que ficaram curiosos sobre as possibilidades de definirmos o conjunto dos números primos, sugerimos o texto

> P. Ribemboin. Existem funções que geram números primos? *Matemática Universitária*. 15, 1–12, 1993.

que pode ser encontrado em

`http://matematicauniversitaria.ime.usp.br/Conteudo/n15/n15_Artigo01.pdf`

4 Definições indutivas

Conjuntos indutivos.

Seja C um conjunto.
Dizemos, grosseiramente, que C é *indutivo* se podemos definir C por indução.

Ou seja, se podemos exibir uma base e um procedimento, tais que todo elemento de C ou pertence à base ou pode ser construído a partir de elementos na base por um número finito de aplicações do procedimento.

Quando definimos um conjunto indutivo, procuramos empregar *bases finitas* que, usualmente, são definidas por listagem e *procedimentos computacionais* que, em princípio, podem ser implementados em um computador.

Exemplo 4.1 (a) *Se admitimos que podemos computar com números reais*, o conjunto $\mathbb{R}^2$, dos vetores do plano de coordenadas reais, é um conjunto indutivo.

De fato, $\mathbb{R}^2$ pode ser definido por indução do seguinte modo:

1. Tome o conjunto $B = \{(0,1),(1,0)\}$, contendo os vetores unitários $(0,1)$ e $(1,0)$, como base.

2. Construa todos os outros elementos de $\mathbb{R}^2$ a partir dos vetores unitários por aplicação iterada das operações $(v,w) \mapsto v+w$, de adição de vetores, e $(\alpha, v) \mapsto \alpha v$, de multiplicação de escalar por vetor (ou seja, todos os vetores de $\mathbb{R}^2$ são combinações lineares de elementos da base).

(b) *Se admitimos que podemos computar com números reais*, o conjunto $\mathbb{R}[x]$, dos polinômios na indeterminada x com coeficientes, é um conjunto indutivo.

De fato, ele pode ser definido por indução do seguinte modo:

1. Tome o conjunto $\mathbb{R} \cup \{x\}$ como base.

2. Construa todos os outros elementos de $\mathbb{R}[x]$ a partir dos elementos da base por aplicação iterada das operações $(p(x), q(x)) \mapsto p(x) + q(x)$, de adição de polinômios, e $(p(x), q(x)) \mapsto p(x) \cdot q(x)$, de multiplicação de polinômios.

Exercício 4.1 No Exemplo 4.1(b) definimos $\mathbb{R}[x]$ pelo procedimento de somar e multiplicar polinômios. Apresente uma definição indutiva alternativa de $\mathbb{R}[x]$ que seja análoga à definição indutiva de $\mathbb{R}^2$ dada no Exemplo 4.1(a), ou seja, apresente uma definição que usa as operações de adição de polinômios e de multiplicação de escalar por polinômio.

Do ponto de vista computacional, qual das duas definições de $\mathbb{R}[x]$ você julga a mais adequada?

Conjuntos indutivos são apresentados através de *definições indutivas*.

Redação de definições indutivas.

Uma *definição indutiva* é um texto escrito estritamente de acordo com as seguintes diretrizes:

– Inicialmente, escrevemos

> Definição.

– Logo em seguida a palavra "Definição.", escrevemos

> Os [nome genérico dos elementos que queremos definir] são os [nome do genérico dos elementos do conjunto universo considerado] obtidos por aplicação das seguintes regras:

– Agora, apresentamos a base, indicando quais são seus elementos.

Podemos escrever frases como:

> Os elementos $b_1, b_2, \ldots, b_n$ são [nome genérico dos elementos que queremos definir]

quando a base é finita e "pequena", ou

> Os [nome genérico dos elementos da base] são [nome genérico dos elementos que queremos definir]
> quando a base é "muito grande" ou infinita.

– No(s) item(ns) seguinte(s), descrevemos o procedimento que pode ser aplicado para a construção dos elementos que queremos definir a partir dos elementos da base.

Usualmente, este procedimento é definido a partir de *operações* que podem ser aplicadas a elementos já definidos para construir novos elementos.

Nestes casos, para cada operação op que pode ser aplicada a, digamos, n elementos $e_1, e_2, \ldots, e_n$ para construir um novo elemento $\mathsf{op}(e_1, e_2, \ldots, e_n)$, podemos escrever frases como:

> Se $x_1, x_2, \ldots, x_n$ são [nome genérico dos elementos que queremos definir] , então $\mathsf{op}(x_1, x_2, \ldots, x_n)$ é um [nome genérico dos elementos que queremos definir]

As variáveis que devem ser utilizadas em frases deste tipo dependem das convenções linguísticas adotadas na teoria que está sendo estudada.

– Finalmente, para encerrar a definição, escrevemos uma frase como:

> Assumimos que nenhum objeto é um [nome genérico dos elementos que queremos definir] a não ser que possa ser obtido por um número finito de aplicações das regras acima.

Para exemplificar a aplicação das diretrizes acima, vamos apresentar definições indutivas dos conjuntos indutivos discutidos na Seção 3.

Definição 4.1 Os *números naturais não nulos* são os números reais obtidos por aplicações das seguintes regras:

1. O número 1 é um número natural não nulo.

2. Se n é um número natural não nulo, então $n + 1$ é um número natural não nulo.

Assumimos que nenhum objeto é um número natural não nulo a não ser que possa ser obtido por um número finito de aplicações das regras acima.

Definição 4.2 Os *números pares não nulos* são os números obtidos por aplicações das seguintes regras:

1. O número 2 é um número par não nulo.

2. Se n é um número par não nulo, então $n + 2$ é um número par não nulo.

Assumimos que nenhum objeto é um número par não nulo a não ser que possa ser obtido por um número finito de aplicações das regras acima.

Definição 4.3 Os *números naturais não nulos* são os números obtidos por aplicações das seguintes regras:

1. Os números primos e o número 1 são números naturais não nulos.

2. Se n e m são números naturais não nulos, então nm é um número natural não nulo.

Assumimos que nenhum objeto é um número natural não nulo a não ser que possa ser obtido por um número finito de aplicações das regras acima.

Exercício 4.2 (i) Escreva uma definição indutiva detalhada do conjunto $\mathbb{I}^*$, de acordo com o Exercício 3.2.
(ii) Escreva uma definição indutiva detalhada do conjunto $\mathbb{R}^2$, de acordo com o Exemplo 4.1(a).
(iii) Escreva uma definição indutiva detalhada do conjunto $\mathbb{R}[x]$, de acordo com o Exemplo 4.1(b).
(iv) Escreva uma definição indutiva detalhada do conjunto $\mathbb{R}[x]$, de acordo com a sua resolução do Exercício 4.1.

5 Provas indutivas

A última condição da definição de um conjunto por indução afirma que nenhum objeto pertence ao conjunto a não ser que seja obtido por um número finito de aplicações das regras estipuladas na definição. Esta condição parece ser desnecessária à primeira vista, mas é essencial e tem como consequência um *método de prova* que pode ser aplicado na prova de que uma dada propriedade é verdadeira para todos os elementos de um conjunto definido por indução.

Método de Prova por Indução, MPI.

Seja C um conjunto definido por indução, cujos elementos são obtidos a partir de uma base, por aplicações sucessivas das operações estipuladas em um procedimento.

Para provar que uma dada propriedade $P(x)$, envolvendo uma variável x que toma elementos de C como valores, é verdadeira para *todos* os elementos de C, basta fazer o seguinte:

1. Provar que $P(x)$ é verdadeira para todos os elementos da base.
2. Para cada operação op que pode ser aplicada a m elementos $e_1, e_2, \ldots, e_m$, previamente definidos, para a construção de um elemento $\mathsf{op}(e_1, e_2, \ldots, e_m)$:
   (a) Supor que $P(x)$ é verdadeira para n elementos arbitrários $x_1, x_2, \ldots, x_n$.
   (b) Provar que $P(x)$ é verdadeira para o elemento arbitrário $\mathsf{op}(x_1, x_2, \ldots, x_n)$, usando a hipótese de que $P(x)$ é verdadeira para $x_1, x_2, \ldots, x_n$.
   As variáveis que devem ser utilizadas nesta parte da prova dependem das convenções linguísticas adotadas na teoria que está sendo estudada.

Para exemplificar o uso do MPI, vamos apresentar provas de algumas propriedades, para os conjuntos definidos por indução nas Seções 3 e 4.

Exemplo 5.1 Baseados na Definição dada no Exemplo 3.1(a), vamos aplicar o MPI para provar a seguinte propriedade:

> Para todo número natural $n \geq 1$, e para todo conjunto A, se A tem n elementos, então $\mathcal{P}(A)$, o conjunto das partes de A, tem 2^n elementos.

Para isto, vamos considerar a propriedade

> $P(n)$: para todo conjunto A, se A tem n elementos, então $\mathcal{P}(A)$ tem 2^n elementos,

sobre números naturais n, e provar que

1. $P(n)$ é verdadeira quando $n = 1$. Ou seja, que para todo conjunto A, se A tem 1 elemento, então $\mathcal{P}(A)$ tem 2^1 elementos.

2. Supor que $P(n)$ é verdadeira para n arbitrário. Ou seja, que para todo conjunto A, se A tem n elementos, então $\mathcal{P}(A)$ tem 2^n elementos.

3. Provar que $P(n)$ é verdadeira para $n+1$, usando a hipótese de que $P(n)$ é verdadeira para n. Ou seja, que para todo conjunto A, se A tem $n+1$ elementos, então $\mathcal{P}(A)$ tem 2^{n+1} elementos.

Como usual, em provas por indução, a prova tem 3 partes, classificadas como *base*, *hipótese* e *passo de indução*.

PROVA. Por indução em n.
Base: Seja A um conjunto arbitrário.

Suponha que A tem 1 elemento.

Ou seja, que $A = \{a_1\}$, onde a_1 é um elemento arbitrário.

Daí, $\mathcal{P}(A) = \{\emptyset, \{a_1\}\}$.

Assim, temos que $\mathcal{P}(A)$ tem 2 elementos.

Logo, $\mathcal{P}(A)$ tem 2^1 elementos.

Hipótese: Suponha que, para todo conjunto A, se A tem n elementos, então $\mathcal{P}(A)$ tem 2^n elementos.

Passo: Seja A um conjunto arbitrário.

Suponha que A tem $n+1$ elementos.

Ou seja, que $A = \{a_1, a_2, \ldots, a_n, a_{n+1}\}$, onde $a_1, a_2, \ldots, a_n, a_{n+1}$ são elementos arbitrários.

Considere $\mathcal{P}(A)$ particionado nos seguintes subconjuntos:

– A família F_1 dos subconjuntos de A que não possuem a_{n+1} como elemento;

– A família F_2 dos subconjuntos de A que possuem a_{n+1} como elemento.

Observe que $F_1 = \mathcal{P}(\{a_1, a_2, \ldots, a_n\})$ e que $\{a_1, a_2, \ldots, a_n\}$ tem n elementos. Logo, pela HI, temos que F_1 tem 2^n elementos.

Agora, para formar um elemento X, de F_2, podemos fazer duas escolhas:

$$\begin{array}{lcl} t_1 & : & \text{escolher } a_{n+1} \text{ para ser elemento de } X \\ t_2 & : & \text{escolher um subconjunto de } \{a_1, a_2, \ldots, a_n\} \\ & & \text{para “completar” a construção de } X \end{array}$$

Temos que t_1 pode ser feita de 1 maneira e, pela HI, que t_2 pode ser feita de 2^n maneiras. Logo, pelo PM, F_2 tem $1 \times 2^n = 2^n$ elementos.

Assim, temos que $\mathcal{P}(A)$ tem $2^n + 2^n = 2 \times 2^n$ elementos.

Logo, $\mathcal{P}(A)$ tem 2^{n+1} elementos. ■

Exercício 5.1 Baseado na Definição dada no Exemplo 3.3(b), aplique o MPI para provar a seguinte propriedade:

Para todo número par $p \geq 2$, temos que p^2 é par.

Exemplo 5.2 Baseados na Definição dada no Exemplo 3.3(b), vamos aplicar o MPI para provar a seguinte propriedade:

Para todo número natural $n \geq 2$, existe um número primo p tal que $p|n$.

Para isto, vamos considerar a propriedade

$P(n)$: existe um número primo p tal que $p|n$,

sobre números naturais n, e provar que

1. $P(n)$ é verdadeira quando $n = 2$. Ou seja, que existe um número primo p tal que $p|2$.
2. Supor que $P(n)$ é verdadeira para m e n arbitrários. Ou seja, que existe um número primo p_1 tal que $p_1|m$ e que existe um número primo p_2 tal que $p_2|n$.
3. Provar que $P(n)$ é verdadeira para $m \times n$, usando a hipótese de que $P(n)$ é verdadeira para m e n. Ou seja, que existe um número primo p tal que $p|n \times m$.

Como usual, em provas por indução, a prova tem 3 partes, classificadas como *base*, *hipótese* e *passo de indução*.

PROVA. Por indução em n.
Base: Para 2, basta considerar $p = 2$.
De fato, temos que 2 é primo e que $2|2$.
Logo, existe um número primo p tal que $p|2$.
Hipótese: Suponha que existe um número primo p_1 tal que $p_1|m$ e que existe um número primo p_2 tal que $p_2|n$.
Passo: Para $m \times n$, basta considerar $p = p_1$.
De fato, temos $p_1|m$ e que $m|m \times n$.
Assim, $p_1|m \times n$.
Logo, existe um número primo p tal que $p|m \times n$. ■

Exercício 5.2 Para os que querem estudar o Método de Indução Matemática (referente a números naturais) um pouco mais profundamente, sugerimos o texto

I.S. Sominski. *Método de Indução Matemática*. Atual e MIR, 1996.

que pode ser vizualizado em

`http://www.scribd.com/doc/27318997/Metodo-de-Inducao-Matematica-Sominski`

6 Legibilidade única

Na Aula 1, vimos que um mesmo conjunto indutivo pode ser definido por indução de mais de uma maneira.

Exemplo 6.1 (a) O conjunto $\mathbb{N}^*$, pode ser definido por indução a partir da base $\{1\}$ por aplicação iterada da operação $n \mapsto n + 1$.

(b) O mesmo conjunto $\mathbb{N}^*$ pode ser definido por indução a partir da base $\{1, 2, 3, 4, 5\}$ por aplicação iterada das operações $n \mapsto n + 1$ e $n \mapsto n + 2$.

(c) O mesmo conjunto $\mathbb{N}^*$ pode ainda ser definido por indução a partir da base $\Pi \cup \{1\}$ por aplicação iterada da operação $(m, n) \mapsto m \times n$, onde Π é o conjunto dos números primos.

Estas definições garantem, respectivamente, que cada número natural não nulo pode ser obtido: (a) a partir do 1 por um número finito de aplicações da operação de somar uma unidade; (b) a partir de $1, 2, 3, 4, 5$ por um número finito de aplicações das operações de somar uma ou duas unidades; (b) a partir do 1 ou de números primos por um número finito de aplicações da operação de multiplicação.

Cada uma destas definições tem os seus méritos e seus deméritos.

Exercício 6.1 Compare as definições por indução de $\mathbb{N}^*$ apresentadas no Exemplo 6.1. Quais são as maiores diferenças que você vê?

Talvez a característica mais importante que diferencia as definições apresentadas nos Exemplos 6.1(a), (b) e (c) seja a maneira como, em cada caso, os elementos são *gerados* a partir da base por aplicações iteradas das operações utilizadas no procedimento.

Exemplo 6.2 Se queremos gerar o número 5 a partir da base $\{1, 2, 3, 4, 5\}$ por aplicação iterada das operações $n \mapsto n + 1$ e $n \mapsto n + 2$, temos várias possibilidades essencialmente distintas.

Podemos, por exemplo, efetuar os seguintes passos:

1. simplesmente, pegar o número 5 na base.

Ou, alternativamente:

1. pegar o número 1 na base;
2. aplicar a operação $n \mapsto n + 1$ ao 1, obtendo o número 2;
3. aplicar a operação $n \mapsto n + 1$ ao 2, obtendo o número 3;

4. aplicar a operação $n \mapsto n+1$ ao 3, obtendo o número 4;

5. aplicar a operação $n \mapsto n+1$ ao 4, obtendo o número 5.

Ou, alternativamente:

1. pegar o número 1 na base;

2. aplicar a operação $n \mapsto n+2$ ao 1, obtendo o número 3;

3. aplicar a operação $n \mapsto n+2$ ao 3, obtendo o número 5.

Ou, alternativamente,

1. pegar o número 2 na base;

2. aplicar a operação $n \mapsto n+2$ ao 2, obtendo o número 4;

3. aplicar a operação $n \mapsto n+1$ ao 4, obtendo o número 5.

E, ainda, outras alternativas que não precisamos considerar.

Esquematicamente, podemos dizer que 5 é gerado, dentre outros, dos seguintes modos

$$5 = 5 = (((1+1)+1)+1)+1 = (1+2)+3 = (2+2)+5$$

a partir de $1, 2, 3, 4, 5$ por aplicações iteradas de $n \mapsto n+1$ e $n \mapsto n+2$ e que estes modos são maneiras essencialmente diferentes de gerar o 5 por este processo.

Exemplo 6.3 Se queremos gerar o número 5 a partir da base $\Pi \cup \{1\}$ por aplicação iterada da operação $(m, n) \mapsto m \times n$, temos algumas possibilidades:

1. simplesmente, pegar o número 5 na base.

Ou, alternativamente,

1. pegar o número 1 na base;

2. pegar o número 5 na base;

3. aplicar a operação $(m, n) \mapsto m \times n$, aos números 1 e 5, obtendo o número 5;

Poderíamos, também, alternativamente, primeiro pegar o 5 na base, depois pegar o 1 na base e, finalmente, multiplicar 1 e 5 obtendo o 5; ou, alternativamente, primeiro pegar o 1 na base, depois pegar o 1 na base novamente, multiplicar 1 e 1 obtendo o 1, depois pegar o 5 na base e, finalmente, multiplicar 1 e 5 obtendo o 5; etc.

Esquematicamente, podemos dizer que 5 é gerado dos seguintes modos

$$5 = 5 = 1 \times 5 = 5 \times 1 = (1 \times 1) \times 5 = \ldots$$

a partir de $\Pi \cup \{1\}$ por aplicações iteradas da operação $(m, n) \mapsto m \times n$.

Observe que, a primeira vista, há infinitas maneiras de gerar o 5 a partir de $\Pi \cup \{1\}$ por multiplicações, mas todas elas envolvem apenas os fatores 1 e 5. Apesar disso, como é usual consideramos que nem as multiplicações por 1 nem as ordens dos fatores diferenciam essencialmente os produtos, podemos dizer, que na verdade existe um único modo de gerar 5 a partir de $\Pi \cup \{1\}$ por aplicações iteradas da operação $(m, n) \mapsto m \times n$. Com isto em mente, podemos dizer esquematicamente que 5 é gerado de uma única maneira:

$$5 = 5$$

Agora, se queremos gerar o número 30 a partir da base $\Pi \cup \{1\}$ por aplicação iterada da operação $(m, n) \mapsto m \times n$, já desconsiderando as multiplicações por 1, aparentemente, também temos algumss possibilidades distintas.

Podemos, por exemplo, efetuar os seguintes passos:

1. pegar os números 2 e 3 na base;
2. aplicar a operação $(m, n) \mapsto m \times n$, aos números 2 e 3, obtendo o número 6;
3. pegar o número 5 na base;
4. aplicar a operação $(m, n) \mapsto m \times n$, aos números 5 e 6, obtendo o número 30.

Ou, alternativamente:

1. pegar os números 2 e 5 na base;
2. aplicar a operação $(m, n) \mapsto m \times n$, aos números 2 e 5, obtendo o número 10;
3. pegar o número 3 na base;
4. aplicar a operação $(m, n) \mapsto m \times n$, aos números 3 e 10, obtendo o número 30.

Ou, alternativamente:

1. pegar os números 3 e 5 na base;
2. aplicar a operação $(m, n) \mapsto m \times n$, aos números 3 e 5, obtendo o número 15;
3. pegar o número 2 na base;
4. aplicar a operação $(m, n) \mapsto m \times n$, aos números 2 e 15, obtendo o número 30.

Esquematicamente, podemos dizer que 30 é gerado de seguintes modos

$$30 = (2 \times 3) \times 5 = (2 \times 5) \times 3 = (3 \times 5) \times 2$$

a partir de $\Pi \cup \{1\}$ por aplicações iteradas da operação $(m, n) \mapsto m \times n$.

Observe que as três maneiras de gerar o 30 a partir de $\Pi \cup \{1\}$ por aplicações iteradas da operação $(m, n) \mapsto m \times n$ apresentadas acima, embora *aparentemente distintas* não são *essencialmente distintas*, uma vez que diferem apenas na ordenação dos números primos que são usados como fatores e não, como no caso do Exemplo 6.2, nos próprios fatores.

Em outras palavras, como é usual consideramos que as ordens dos fatores não diferenciam essencialmente os produtos, podemos dizer, que na verdade existe um único modo de gerar 30 a partir de $\Pi \cup \{1\}$ por aplicações iteradas da operação $(m, n) \mapsto m \times n$. Ou seja, podemos dizer esquematicamente que 30 é gerado de uma única maneira:

$$30 = 2 \times 3 \times 5$$

Desde os nossos contatos iniciais com a Matemática — particularmente, quando aprendemos a fatorar números naturais — somos levados a perceber que a observação acima não é uma propriedade exclusiva nem do 5 nem do 30 e vale para qualquer número natural não nulo n. Esta propriedade geral é chamada de *Teorema Fundamental da Aritmética* e, para os nossos propósitos pode ser enunciada do seguinte modo:

> Para qualquer número natural não nulo n, ou $n = 1$, ou existem números primos $p_1 < p_2 < \ldots < p_m$ e números naturais $\alpha_1, \alpha_2, \ldots, \alpha_m$, univocamente determinados, tais que n "pode ser escrito" do seguinte modo
>
> $$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}$$

Isto é, n pode ser gerado a partir de $\Pi \cup \{1\}$ por aplicações iteradas da operação $(m, n) \mapsto m \times n$ e, se desconsideramos as multiplicações por 1 e a ordem dos fatores, existe uma única maneira de gerar n por este processo.

Exemplo 6.4 Agora, se queremos gerar o número 5 a partir da base $\{1\}$ por aplicação iterada da operação $n \mapsto n + 1$, temos necessariamente que efetuar os seguintes passos:

1. pegar o número 1 na base;
2. aplicar a operação $n \mapsto n + 1$ ao 1, obtendo o número 2;
3. aplicar a operação $n \mapsto n + 1$ ao 2, obtendo o número 3;
4. aplicar a operação $n \mapsto n + 1$ ao 3, obtendo o número 4;
5. aplicar a operação $n \mapsto n + 1$ ao 4, obtendo o número 5.

Esquematicamente, podemos dizer que 5 é gerado do seguinte modo

$$5 = (((1 + 1) + 1) + 1) + 1$$

a partir do 1 por aplicações iteradas de $n \mapsto n + 1$ e que este é o único modo de gerar 5 por este processo.

Intuitivamente, percebemos que a observação acima não é uma propriedade exclusiva do 5 e vale para qualquer número natural n. Esta propriedade geral é chamada de *Teorema da Legibilidade Única* e, para os nossos propósitos pode ser enunciada do seguinte modo:

> Para qualquer número natural não nulo n, temos que n pode ser gerado a partir de $\{1\}$ por aplicações iteradas da operação $n \mapsto n+1$ do seguinte modo
>
> $$n = \underbrace{(((1+1)+1)+1)+\ldots+1}_{n \text{ vezes}}$$
>
> e este é o único modo de gerar n por este processo.

A partir da distinção apontada acima é natural classificarmos as definições por indução em duas categorias:

1. aquelas em que cada elemento do conjunto definido é gerado de uma única maneira a partir dos elementos básicos pelo procedimento de geração de elementos;
2. aquelas em que existem elementos do conjunto definido que podem ser gerados de mais de uma maneira a partir dos elementos básicos pelo procedimento de geração de elementos.

Legibilidade única.

Seja C um conjunto indutivo, definido a partir de uma base por aplicação de um procedimento.
Dizemos, grosseiramente, que esta definição de C tem *legibilidade única* se cada elemento de C é gerado de uma única maneira a partir dos elementos básicos pelo procedimento de geração de elementos.

Exercício 6.2 Para cada definição abaixo, determine se há legibilidade única.

(i) O conjunto $\mathbb{P}^*$, dos números pares não nulos, a partir da base $\{2\}$ por aplicação iterada da operação $n \mapsto n+2$.

(ii) O conjunto $\mathbb{I}^*$, dos números ímpares não nulos, de acordo com a definição que você apresentou na resolução do Exercício 3.2 da Aula 1.

(iii) O conjunto $\mathbb{R}^2$, dos vetores no plano, a partir da base $B = \{(0,1),(1,0)\}$ por aplicação iterada das operações $(v,w) \mapsto v+w$ e $(\alpha, v) \mapsto \alpha v$.

(iv) O conjunto $\mathbb{R}[x]$, dos polinômios na indeterminada x com coeficientes reais, a partir da base $\mathbb{R} \cup \{x\}$ por aplicação iterada das operações $(p(x), q(x)) \mapsto p(x)+q(x)$ e $(p(x), q(x)) \mapsto p(x) \cdot q(x)$.

(v) O conjunto $\mathbb{R}[x]$, dos polinômios na indeterminada x com coeficientes reais, de acordo com a definição que você apresentou na resolução do Exercício 4.1 da Aula 1.

Nós não vamos nos aprofundar nos estudos das definições indutivas com legibilidade única — embora esta noção seja essencial na Teoria da Computação, por exemplo, na definição das Linguagens de Programação. Até o momento, a única coisa importante é que você tenha em mente que esta noção existe e que tenha conseguido aplicá-la na resolução dos exercícios acima.

7 Definições recursivas

Assim como definições por indução levam a um *método de prova* de proposições que valem para todos os elementos do conjunto definido — ou seja, todo conjunto indutivo tem um método de prova associado — as definições por indução que têm legibilidade única levam a um *método de definição* de conceitos que podem ser aplicados a todos os elementos do conjunto definido.

Intuitivamente, a ideia é a seguinte:

> Seja C um conjunto indutivo definido por uma definição indutiva que tem legibilidade única.
>
> Para definir um conceito para *todas* os elementos de C, basta fazer o seguinte:
>
> 1. Definir o conceito para todos os elementos da base.
> 2. Para cada operação op que pode ser aplicada a, digamos, n elementos $e_1, e_2, \ldots, e_n$ para construir um novo elemento $\mathsf{op}(e_1, e_2, \ldots, e_n)$, fazer o seguinte:
>
>   Supondo que o conceito está definido para os elementos genéricos $x_1, x_2, \ldots, x_n$, mostrar como o conceito é definido para o elemento genérico $\mathsf{op}(x_1, x_2, \ldots, x_n)$, usando as definições para $x_1, x_2, \ldots, x_n$.

Para exemplificar como a ideia acima é aplicada, vamos apresentar definições recursivas a partir das definições apresentadas nos Exemplos 6.1(a) e 6.1(c), que possuem a propriedade da legibilidade única (esta última, se ordenamos a maneira como os elementos são tomados na base).

Exemplo 7.1 (a) O fatorial de um número natural n é o número $n!$ obtido pela multiplicação de todos os números naturais de 1 a n. Por exemplo, $1! = 1$, $2! = 1 \times 2 = 2$, $3! = 1 \times 2 \times 3 = 6$, $4! = 1 \times 2 \times 3 \times 4 = 24$, $5! = 1 \times 2 \times 3 \times 4 \times 5 = 120$, etc.

De acordo com a definição apresentada no Exemplo 6.1(a), este conceito pode ser definido do seguinte modo:

Definição 7.1 Seja $n \in \mathbb{N}^*$. O *fatorial de* n, denotado por $n!$, é definido recursivamente pelas seguintes regras:

1. Se $n = 1$, então $n! = 1$.

2. Se $n = m + 1$, então $n! = (m + 1) \times m!$.

Observe que na definição acima, determinamos diretamente o valor do fatorial de 1 e mostramos como o fatorial de $m + 1$ pode ser calculado a partir do fatorial de m.

(b) Seja $n \in \mathbb{N}^*$. Dizemos que um número é primo com n se ele e n não têm fatores primos em comum. Por exemplo, para $n = 2$, temos 1 é primo com 2, 2 não é primo com 2, 3 é primo com 2, 4 não é primo com 2, 5 é primo com 2, etc.

De acordo com a definição apresentada no Exemplo 6.1(c), este conceito pode ser definido do seguinte modo:

Definição 7.2 Seja $n \in \mathbb{N}^*$. Dado $m \in \mathbb{N}^*$, o conceito m *é primo com* n, denotado $m \perp n$, é definido recursivamente pelas seguintes regras:

1. Se $m = 1$, ent ao $m \perp n$.

2. Se $m \in \Pi$, então $m \perp n$ se, e somente se, $m \neq n$.

3. Se $m = m_1 \times m_2$, então: $m \perp n$ se, e somente se, $m_1 \perp n$ e $m_2 \perp n$.

Observe que na definição acima, determinamos diretamente que 1 é primo com n e quando um número primo p é primo com n; e mostramos como determinar se um produto $m_1 \times m_2$ é primo com n, dado que sabemos determinar se m_1 e m_2 são primos com n.

Conceitos definidos por recursão são apresentados através de *definições recursivas*. Estas definições são textos razoavelmente elaborados que devem ser escritos de maneira uniforme, conforme as diretrizes abaixo. Estas diretrizes conferem um certo grau de liberdade na escolha das palavras e notações usadas na definição, mas devem ser seguidas estritamente, tanto quanto possível.

Redação de definições recursivas.

Uma *definição recursiva* é um texto escrito estritamente de acordo com as seguintes diretrizes:

– Inicialmente, escrevemos

> Definição.

– Logo em seguida a palavra "Definição.", escrevemos uma frase como:

> Seja x um elemento de C.

A variável que deve ser utilizada em frases deste tipo depende das convenções linguísticas adotadas na teoria que está sendo estudada.

– Agora, escrevemos uma frase como:

> O [nome do conceito que está sendo definido], denotado por [notação introduzida para referência ao conceito que está sendo definido], é definido recursivamente pelas seguintes regras:

Sempre que possível, a notação introduzida deve ser adaptada de e compatível com as outras notações da teoria que está sendo estudada.

– Agora, definimos o conceito para os elementos da base.

Podemos escrever frases como:

> Se x está em B, então [descrição do conceito que queremos definir aplicado a x, usando a notação introduzida acima].

– No(s) item(ns) seguinte(s), descrevemos o procedimento que pode ser aplicado para a construção dos elementos que queremos definir a partir dos elementos previamente definidos.

Usualmente, este procedimento é especificado a partir de *operações* que podem ser aplicadas a elementos já definidos para construir novos elementos.

Nestes casos, para cada operação op que pode ser aplicada a, digamos, n elementos $e_1, e_2, \ldots, e_n$ para construir um novo elemento $\mathsf{op}(e_1, e_2, \ldots, e_n)$, podemos escrever frases como:

> Se $x = \mathsf{op}(x_1, x_2, \ldots, x_n)$, então [descrição do conceito que queremos definir aplicado a x, usando a notação introduzida acima, baseada na definição do conceito para $x_1, x_2, \ldots, x_n$].

As variáveis que devem ser utilizadas em frases deste tipo dependem das convenções linguisticas adotadas na teoria que está sendo estudada.

Exercício 7.1 Baseado na definição apresentada no Exemplo 6.1(a) e nas diretrizes de redação de definições recursivas, defina os seguintes conceitos por recursão:

(i) O dobro de um número natural n, denotado $\mathsf{D}(n)$.

(ii) A paridade de um número natural n, denotada $\mathsf{P}(n)$.
Informamos que a paridade de um número natural n é definida (não por recursão é claro), do seguinte modo:

$$\mathsf{P}(n) = \begin{cases} 0 & \text{se } n \text{ é par} \\ 1 & \text{se } n \text{ é ímpar} \end{cases}$$

Um último comentário é que, talvez, não esteja clara a necessidade da legibilidade única para o processo de definição por recursão. Apenas para ilustrar este ponto, vamos considerar a definição recursiva de um conceito (um tanto artificial) sobre números naturais não nulos a partir da definição apresentada no Exemplo 6.1(b).

Exemplo 7.2 Suponhamos que queiramos definir o número de parcelas de um número natural não nulo, de acordo com a definição apresentada no Exemplo 6.1(b).

De acordo com esta definição é natural que definamos o conceito do seguinte modo:

Definição 7.3 Seja $n \in \mathbb{N}^*$. O *número de parcelas de* n, denotado por $\mathsf{NP}(n)$, é definido recursivamente pelas seguintes regras:

1. Se $n = 1$, então $\mathsf{MP}(n) = 1$.
2. Se $n = 2$, então $\mathsf{MP}(n) = 1$.
3. Se $n = 3$, então $\mathsf{MP}(n) = 1$.
4. Se $n = 4$, então $\mathsf{MP}(n) = 1$.
5. Se $n = 5$, então $\mathsf{MP}(n) = 1$.
6. Se $n = m + 1$, então $\mathsf{NP}(n) = \mathsf{NP}(m) + 1$.
7. Se $n = m + 2$, então $\mathsf{NP}(n) = \mathsf{NP}(m) + 1$.

Observe que na definição acima, determinamos diretamente o valor dos números de parcelas de $1, 2, 3, 4, 5$, e mostramos como os números de parcelas de $m + 1, m + 2$ podem ser calculados a partir do número de parcelas de m.

Aparentemente, tudo está perfeito! Mas, vejamos o que acontece quando aplicamos a definição acima no cálculo de números de parcelas.

Por exemplo, para calcular $\mathsf{NP}(5)$, teríamos várias possibilidades, de acordo com a maneira como geramos 5 a partir da base:

$$\begin{array}{lcl} 5 = 5 & \Rightarrow & \mathsf{NP}(5) = 1 \\ 5 = 4 + 1 & \Rightarrow & \mathsf{NP}(5) = \mathsf{NP}(4) + 1 = 1 + 1 = 2 \end{array}$$

Em resumo,

quando não temos legibilidade única, ao aplicarmos (indevidamente) o Método de Definição por Recursão a um conceito, o conceito pode não estar bem definido, pois seu valor pode depender da maneira como consideramos a geração do elemento a partir da base.

Por outro lado,

quando temos um conjunto indutivo definido por uma definição indutiva que tem legibilidade única, podemos definir um conceito sobre os elementos do conjunto, simplesmente (1) explicando o conceito na base; (2) assumindo que o conceito está definido para os elementos genéricos obtidos do conjunto; e (3) explicando como o conceito está definido para os elementos genŕicos obtidos a partir de elementos anteriores, para os quais o conceito já está presumivelmente definido.

Exercício 7.2 (i) Baseado na definição apresentada na resolução do Exercício 7.1(i), prove por indução que o dobro de um número natural não nulo é um número par.

(iii) Baseado na definição apresentada no Exemplo 6.1(b) e nas diretrizes de redação de definições recursivas, defina o fatorial de um número natural e prove por indução que a definição apresentada calcula o fatorial corretamente.

Mais exercícios

1. Escreva uma definição por indução para cada um dos seguintes conjuntos. Isto é, em cada caso, explicite um conjunto base e descreva um procedimento para gerar todos os elementos do conjunto a partir dos elementos básicos.

   (a) $M(3) = \{x \in \mathbb{N}^* : x \text{ é múltiplo de } 3\}$

   (b) O conjunto dos números inteiros, $\mathbb{Z}$.

   (c) $\left\{ \frac{1}{2^n} : n \in \mathbb{N}^* \right\} \subseteq \mathbb{R}$.

(d) $G = \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \ \cdots \right\}$.

2. Que conjunto é definido indutivamente considerando-se a base $\{2\}$ e o procedimento de, dado um número natural não nulo, multiplicá-lo por 2 (ou seja, a operação $n \mapsto 2n$)?

3. Considerando as definições indutivas apresentadas no Exercício 1, apresente provas por indução para os seguintes enunciados:

   (a) Para todo $n \in M(3)$, a soma dos algarismos de n é um múltiplo de 3.

   (b) Para todo número inteiro a, temos que $a^2 + a$ é divisível por 2.

   (c) Para toda matriz $M_{m\times n} \in G$, temos que $m = 2^n$.

4. Considerando a definição indutiva usual do conjunto dos números naturais não nulos, apresentada na Aula 1 (Definição 4.1), apresente definições recursivas dos conceitos a seguir.

   (a) O triplo de um natural não nulo, $3n$.

   (b) O quádruplo de um natural não nulo, $5n$.

   (c) Dado a um natural não nulo, o produto de a por um natural não nulo, an.

   (d) Dado a um natural não nulo, a n-ésima potência de base a, onde n é um natural não nulo, a^n.

5. Considerando as definições apresentadas no item anterior, apresente provas por indução para as proposições a seguir.

   (a) Para todos os naturais não nulos m e n, temos que $mn = nm$.

   (b) Para todos os naturais não nulos a, b e c, temos que $a(b + c) = ab + ac$.

   (c) Para todos os naturais não nulos a, m e n, temos que $a^m a^n = a^{m+n}$.

   (d) Para todos os naturais não nulos a, m e n, temos que $(a^m)^n = a^{mn}$.

6. Considerando a definição indutiva do conjunto dos números naturais não nulos que tem o conjunto dos números primos e a unidade como base e a multiplicação como procedimento gerador, apresentada na Aula 1 (Definição 4.3), apresente definições recursivas dos conceitos a seguir.

(a) Dado a um natural não nulo, o máximo divisor comum entre a e um natural não nulo, $\mathsf{mdc}(a, n)$.

(b) Dado a um natural não nulo, o mínimo múltiplo comum entre a e um natural não nulo, $\mathsf{mmc}(a, n)$.

(c) A condição de divisibilidade entre naturais não nulos, $m \mid n$.

7. Considerando as definições apresentadas no item anterior, apresente provas por indução para as proposições a seguir.

(a) Para todos os naturais não nulos m e n, temos que

$$\mathsf{mdc}(m, n) = \mathsf{mdc}(n, m).$$

(b) Para todos os naturais não nulos m e n, temos que

$$\mathsf{mmc}(m, n) = \mathsf{mmc}(n, m).$$

(c) Para todos os naturais não nulos m e n, temos que $\mathsf{mdc}(m, n) \mid m$.

(d) Para todos os naturais não nulos m e n, temos que $m \mid \mathsf{mmc}(m, n)$.

IME-UFF, Niterói, RJ