Lógica CC
Licenciatura em Ciências da Computação

Luís Pinto

Departamento de Matemática
Universidade do Minho

1º. semestre, 2020/2021

1. Preliminares: definições indutivas e linguagens

Exemplo 1: Seja C o menor[1] subconjunto de $\mathbb{N}_0$ que satisfaz as seguintes condições:

1. $0 \in C$;
2. para todo $n \in \mathbb{N}_0$, se $n \in C$, então $n+2 \in C$.

[1] Dizemos que um conjunto A é mais pequeno que um conjunto B quando $A \subseteq B$.

Exemplo 1 (cont.):

Exemplos de elementos de C são: 0, 2, 4.

De facto:

- 0 é um elemento de C, por C satisfazer 1;
- sabendo que $0 \in C$, por C satisfazer 2, segue $0 + 2 = 2 \in C$;
- sabendo que $2 \in C$, por C satisfazer 2, segue $2 + 2 = 4 \in C$.

Exemplo 1 (cont.):

Adiante (e como é fácil de intuir), mostraremos que C é o conjunto dos números pares.

Esta forma de definir o conjunto C é um caso particular das chamadas *definições indutivas de conjuntos*, um mecanismo muito útil para definir conjuntos (e de uso frequente em Ciências de Computação), que apresentaremos de seguida.

Definição 2: Sejam X um conjunto e B um subconjunto não vazio de X. Seja O um conjunto de *operações* em X (*i.e.*, funções do tipo $X^n \longrightarrow X$, com $n \in \mathbb{N}$).

Um subconjunto I de X tal que

i) $B \subseteq I$ e

ii) I é *fechado* para as operações de O (*i.e.*, as operações de O quando aplicadas a elementos de I produzem elementos de I ou, por outras palavras, para cada operação $f : X^n \longrightarrow X$ de O e para cada $(x_1, ..., x_n) \in I^n$, $f(x_1, ..., x_n) \in I$)

é chamado um *conjunto indutivo*, sobre X, *de base B* e *conjunto de operações O*.

Observação 3: Admitamos as suposições da definição anterior. Então:

i) X é um conjunto indutivo para qualquer O;

ii) B é um conjunto indutivo quando $O = \emptyset$.

Donde, podemos concluir que os subconjuntos indutivos de um conjunto, para uma dada base e um dado conjunto de operações, não são necessariamente únicos, pois X e B são ambos conjuntos indutivos, sobre X, de base B e conjunto de operações $\emptyset$.

Definição 4: Sejam X um conjunto, B um subconjunto não vazio de X e O um conjunto de *operações* em X.

O menor conjunto indutivo, sobre X, de base B e conjunto de operações O é chamado o *conjunto definido indutivamente* (ou *conjunto gerado*) por O em B. Chamaremos ao par (B, O) uma *definição indutiva sobre o conjunto suporte X*.

Exercício 5: Explicite X, B e O no caso do conjunto definido indutivamente no exemplo inicial.

Observação 6: Nas condições da definição anterior, demonstra-se que o conjunto G gerado por O em B é a interseção de todos os conjuntos indutivos, sobre X, de base B e conjunto de operações O.

Alternativamente, demonstra-se que os elementos de G são exatamente os objetos que podem ser obtidos a partir de B, aplicando um número finito de operações de O.

Definição 7:

1. Chamaremos *alfabeto* a um conjunto de símbolos e chamaremos *letras* aos elementos de um alfabeto.
2. Dado um alfabeto A, chamaremos *palavra* (ou *string*) sobre o alfabeto A a uma sequência finita de letras de A.

   A notação A^* representará o conjunto de todas as palvras sobre A.

Definição 7 (cont.):

3. À sequência vazia de letras de A chamaremos *palavra vazia*, notando-a por ϵ.

4. Dado $n \in \mathbb{N}$ e dadas n letras a_1, a_2, ..., a_n de um alfabeto A (possivelmente com repetições), utilizamos a notação $a_1 a_2 \ldots a_n$ para representar a palavra sobre A cuja i-ésima letra (para $1 \leq i \leq n$) é a_i.

Definição 7 (cont.):

5. O *comprimento de uma palavra* é o comprimento da respetiva sequência de letras.

   Em particular, a única palavra de comprimento 0 é ϵ.

   Dada uma palavra u, denotamos por $|u|$ o comprimento de u.

6. Duas *palavras* sobre um alfabeto dizem-se *iguais* quando têm o mesmo comprimento e coincidem letra a letra.

Definição 7 (cont.):

7. Dadas duas palavras u, v sobre um alfabeto, utilizamos a notação uv para representar a *concatenação de u com v* (*i.e.*, a concatenação das respetivas sequências de letras, colocando primeiro a sequência de letras relativa a u).

8. Uma *linguagem sobre um alfabeto A* é um conjunto de palavras sobre A (i.e. um subconjunto de A^*).

Exemplo 8: Seja A o alfabeto $\{0, s, +, \times, (,)\}$. Consideremos a linguagem *E* em A (E para *expressões*), definida indutivamente pelas seguintes *regras*:

1. $0 \in E$;
2. $e \in E \Rightarrow s(e) \in E$, para todo $e \in A^*$;
3. $e_1, e_2 \in E \Rightarrow (e_1 + e_2) \in E$, para todo $e_1, e_2 \in A^*$;
4. $e_1, e_2 \in E \Rightarrow (e_1 \times e_2) \in E$, para todo $e_1, e_2 \in A^*$.

Exemplo 8 (cont.):

Por exemplo, as palavras 0, $s(0)$, (0×0), $(s(0) + (0 \times 0))$ pertencem a E.

De facto:

- $0 \in E$, pela regra 1;
- de $0 \in E$, pela regra 2, segue $s(0)$;
- de $0 \in E$, pela regra 4, segue (0×0);
- de $s(0) \in E$ e (0×0), pela regra 3, segue $(s(0) + (0 \times 0))$.

Exemplo 8 (cont.):

Já as palavras sobre A $+(00)$ e $s0$ não pertencem a E.

Note-se que nenhuma palavra de E tem a letra $+$ como primeira letra e nenhuma palavra de E, com exceção da palavra 0, tem 0 como última letra.

Definição 9: Seja (B, O) uma definição indutiva sobre um conjunto suporte X de um conjunto I e seja $e \in X$.

Uma *sequência de formação de e* é uma sequência finita de elementos de X na qual:

1. o último elemento é e;
2. cada elemento pertence a B ou é imagem de elementos anteriores na sequência por uma operação de O.

Na representação de uma sequência de formação, habitualmente, usaremos vírgulas para separar os elementos da sequência.

Exemplo 10: Retomemos o exemplo anterior.

A sequência de 4 palavras

$$0, s(0), (0 \times 0), (s(0) + (0 \times 0))$$

é uma sequência de formação de $(s(0) + (0 \times 0))$. Porquê?

Esta sequência de formação representa o essencial da justificação que apresentámos no Exemplo 8 para provar que $(s(0) + (0 \times 0))$ é uma palavra da linguagem E.

Proposição 11: Seja I um conjunto definido indutivamente, sobre um conjunto suporte X, e seja $e \in X$. Então, e é um dos elementos de I se e somente se e admite uma sequência de formação.

Observação 12: Retomemos o Exemplo 10.

A sequência de formação de $(s(0) + (0 \times 0))$ que aí apresentamos não é única.

Por exemplo,

$$0, (0 \times 0), s(0), (s(0) + (0 \times 0))$$

é também uma sequência de formação de $(s(0) + (0 \times 0))$. Porquê?

Exemplo 8 (cont.):

Na verdade, quando um objeto tem uma sequência de formação, esse objeto admite uma infinidade de sequências de formação.

Por exemplo, no caso anterior, podemos aumentar o comprimento da sequência acima, tanto quanto queiramos, adicionando 0's no início da sequência.

Observação 13: A demonstração da Proposição 11, em particular, requer a ferramenta de *indução estrutural*, que estudaremos de seguida.

Teorema 14 (Princípio de indução estrutural associado a uma definição indutiva):

Considere-se uma definição indutiva (B, O) de um conjunto I sobre X e seja $P(e)$ uma condição sobre $e \in I$.

Se:

1. para todo $b \in B$, $P(b)$ é verdadeira;
2. para cada operação $f : X^n \to X$ de O, para todo $e_1, ..., e_n \in I$, se $P(e_1), \ldots P(e_n)$ são verdadeiras, então $P(f(e_1, \ldots, e_n))$ é verdadeira;

então, para todo $e \in I$, $P(e)$ é verdadeira.

Dem.:

Seja $Y = \{e \in I : P(e) \text{ é verdadeira}\}$.

Então, Y é um conjunto indutivo, pois contém B e é fechado para as operações de O.

Logo, como I é o menor dos conjuntos indutivos, $I \subseteq Y$.

Como da definição de Y se tem também $Y \subseteq I$, segue que $Y = I$.

Portanto, por definição de Y, tem-se que, para todo $e \in I$, $P(e)$ é verdadeira. $\square$

Observação 15:

1. A cada definição indutiva de um conjunto I está associado um princípio de indução estrutural.

2. O usual Princípio de indução sobre os naturais é o princípio de indução estrutural associado à seguinte caracterização indutiva de $\mathbb{N}$:

   $\mathbb{N}$ é o menor subconjunto de $\mathbb{N}$ que satisfaz as seguintes condições:

   1. $1 \in \mathbb{N}$;
   2. para todo $n \in \mathbb{N}$, se $n \in \mathbb{N}$, então $n + 1 \in \mathbb{N}$.

Exemplo 16: O Princípio de indução estrutural associado à definição indutiva do conjunto C do Exemplo 1 é o seguinte:

Seja $P(n)$ uma condição sobre $n \in C$. Se:

1. $P(0)$;
2. se $P(k)$, então $P(k+2)$, para todo $k \in C$;

então, $P(n)$ é verdadeira, para todo $n \in C$.

Exemplo 16 (cont.):

Consideremos a condição $P(n)$, com $n \in C$, dada por: "n é par".

Provemos que $P(n)$ é verdadeira, para todo $n \in C$.

Pelo Princípio de indução estrutural para C, basta mostrar que as duas condições acima são verificadas.

1. 0 é par. Logo, $P(0)$ é verdadeira.
2. Seja $k \in C$. Suponhamos que $P(k)$ é verdadeira. Então, k é par. Logo, $k + 2$ é também par e, portanto, $P(k + 2)$ é verdadeira. Provámos, assim, a condição 2 do Princípio de indução estrutural para C.

Exemplo 16 (cont.):

Para mostar que C é efetivamente o conjunto dos números pares, falta ainda mostrar que C contém o conjunto dos números pares.

Para tal, pode provar-se, por indução em $\mathbb{N}_0$, que, para todo $n \in \mathbb{N}_0$, $2n \in C$. (Exercício.)

Exemplo 17: O Princípio de indução estrutural associado à definição indutiva da linguagem de expressões E do Exemplo 8 é o seguinte:

Seja $P(e)$ uma condição sobre $e \in E$.

Se:

1. $P(0)$;
2. se $P(e)$, então $P(s(e))$, para todo $e \in E$;
3. se $P(e_1)$ e $P(e_2)$, então $P((e_1 + e_2))$, para todo $e_1, e_2 \in E$;
4. se $P(e_1)$ e $P(e_2)$, então $P((e_1 \times e_2))$, para todo $e_1, e_2 \in E$;

então $P(e)$, para todo $e \in E$.

Exemplo 18: Consideremos de novo a linguagem de expressões E do Exemplo 8 .

Consideremos a função $np : E \longrightarrow \mathbb{N}_0$ que, a cada expressão de E, faz corresponder o número de ocorrências de parênteses na expressão.

Esta função pode ser definida por *recursão estrutural em E* do seguinte modo:

1. $np(0) = 0$;
2. para todo $e \in E$, $np(s(e)) = 2 + np(e)$;
3. para todo $e_1, e_2 \in E$, $np((e_1 + e_2)) = 2 + np(e_1) + np(e_2)$;
4. para todo $e_1, e_2 \in E$, $np((e_1 \times e_2)) = 2 + np(e_1) + np(e_2)$.

Exemplo 18 (cont.): Recordemos a definição da função *np*:

1. $np(0) = 0$;
2. para todo $e \in E$, $np(s(e)) = 2 + np(e)$;
3. para todo $e_1, e_2 \in E$, $np((e_1 + e_2)) = 2 + np(e_1) + np(e_2)$;
4. para todo $e_1, e_2 \in E$, $np((e_1 \times e_2)) = 2 + np(e_1) + np(e_2)$.

Notemos que, nos casos relativos às regras indutivas de E (casos 2, 3 e 4), a caracterização da imagem é feita em termos da imagem da *subexpressão direta* (caso 2) ou das imagens das *subexpressões diretas* (casos 3 e 4).

Exemplo 18 (cont.):
Mostremos, agora, uma das propriedades das expressões de E relativa à função np.

Designadamente, mostremos que, para todo $e \in E$, $np(e)$ é par.

A prova será feita com recurso ao Princípio de indução estrutural para E, descrito no exemplo anterior.

Para cada $e \in E$, seja $P(e)$ a afirmação "$np(e)$ é par".

1. $P(0)$ é a afirmação "$np(0)$ é par".

   Ora, $np(0) = 0$, que, evidentemente, é par.

   Logo, $P(0)$ é verdadeira.

Exemplo 18 (cont.):

2. Seja $e \in E$ e suponhamos que $P(e)$ é válida (a hipótese de indução (H.I.)). Ou seja, suponhamos que $np(e)$ é par.

   Queremos provar que $P(s(e))$ é válida, i.e., que $np(s(e))$ é par.

   Ora, $np(s(e)) = 2 + np(e)$.

   Sendo $np(e)$ par, por H.I., e sendo a soma de dois pares um par, é óbvio que também $np(s(e))$ é par.

   Logo, podemos deduzir que $P(s(e))$ é válida.

Exemplo 18 (cont.):

3. Sejam $e_1, e_2 \in E$ e suponhamos que $P(e_1)$ e $P(e_2)$ são válidas (as hipóteses de indução (H.I.)). Ou seja, suponhamos que $np(e_1)$ é par, assim como $np(e_2)$.

   Queremos provar que $P((e_1 + e_2))$ é válida, i.e., que $np(e_1 + e_2)$ é par.

   Note-se que $np((e_1 + e_2)) = 2 + np(e_1) + np(e_2)$.

   Por H.I., sabemos que $np(e_1)$ e $np(e_2)$ são pares.

   Como a soma de pares é também par, é claro que $np((e_1 + e_2))$ é par.

   Assim, pode-se concluir que $P((e_1 + e_2))$ é válida.

Exemplo 18 (cont.):

4. Sejam $e_1, e_2 \in E$ e suponhamos que $P(e_1)$ e $P(e_2)$ são válidas (H.I.).

   Logo, $np(e_1)$ e $np(e_2)$ são pares.

   Queremos mostrar que $P((e_1 \times e_2))$ é válida, ou seja, que $np(e_1 \times e_2)$ é par.

   Temos que $np((e_1 \times e_2)) = 2 + np(e_1) + np(e_2)$.

   Ora, sabemos, por H.I., que $np(e_1)$ e $np(e_2)$ são pares.

   Consequentemente, $np((e_1 \times e_2))$ é par.

   Assim, podemos afirmar que $P((e_1 \times e_2))$ é válida.

Exemplo 18 (cont.):

Mostrámos assim que as condições 1, 2, 3 e 4 do Princípio de indução estrutural para E são verificadas.

Logo, por esse princípio, conclui-se que $P(e)$ é verdadeira, para todo o $e \in E$, ou seja, que $np(e)$ é par, para todo o $e \in E$.

Exemplo 19: A definição indutiva do conjunto C do Exemplo 1 também permite a definição de funções por recursão estrutural.

Por exemplo, existe uma e uma só função $f : C \longrightarrow \mathbb{N}_0$ que satisfaz as seguintes condições:

1. $f(0) = 0$;
2. para todo $n \in C$, $f(n+2) = 1 + f(n)$.

Acerca desta função, pode provar-se, com recurso ao Princípio de indução para C (ver Exemplo 1), que, para todo $n \in C$, $f(n) = \frac{n}{2}$. (Exercício.)

Observação 20:

Ao contrário do que sucede em relação ao *Princípio de indução estrutural*, nem todas as definições indutivas têm um *Princípio de recursão estrutural* associado.

Este princípio é válido apenas para as chamadas *definições indutivas deterministas*.

As definições indutivas de C e E, que vimos nos Exemplos 1 e 8, inserem-se nesta classe.

As definições indutivas deterministas caracterizam-se por permitirem *decomposições únicas dos elementos* nos conjuntos por si gerados.

Observação 20 (cont.): Vejamos um exemplo de uma definição indutiva não-determinista e de problemas que surgiriam com um hipotético princípio de recursão estrutural associado.

Tomemos a definição indutiva de C do Exemplo 1 e acrescentemos-lhe, agora, a regra:

3. para todo $n \in \mathbb{N}_0$, se $n \in C$, então $2 \times n \in C$.

Simultaneamente, às condições que definem a função f, no exemplo anterior, acrescentemos, agora, a seguinte condição associada à regra que acabámos de introduzir:

3. para todo $n \in C$, $f(2n) = 2 + f(n)$.

O princípio de recursão estrutural associado asseguraria que esta condição, juntamente com as condições 1 e 2 do exemplo anterior, definiriam uma função.

Observação 20 (cont.):

Mas, por exemplo, qual seria a imagem de 4 por f?

Por um lado,
$f(4) = f(2 \times 2) = 2 + f(2) = 2 + f(2+0) = 2 + 1 + f(0) = 3 + 0 = 3$
(fazendo na primeira igualdade a *decomposição de* 4 *pela regra* 3 e usando a condição 3 na segunda igualdade).

Por outro lado,
$f(4) = f(2 + 2) = 1 + f(2) = 1 + 1 = 2$
(fazendo na primeira igualdade a *decomposição de* 4 *pela regra* 2 e usando a condição 2 na segunda igualdade).

Teríamos, portanto, duas imagens distintas para 4, o que é impossível.

Consequentemente, o princípio de recursão estrutural não pode ser válido para esta definição indutiva.