Noções básicas de álgebra universal para a disciplina de Fundamentos Algébricos de Engenharia da Programação da LMAC

PEDRO RESENDE

Departamento de Matemática
Instituto Superior Técnico

Conteúdo

1 Álgebras

Seja A um conjunto. Uma *operação sobre* A é uma função $f : A^n \to A$, onde n é um número natural, dito a *aridade* da operação. Operações de aridade zero são denominadas *constantes* de A.

Uma *álgebra* consiste num conjunto A, também denominado *domínio* ou *suporte* da álgebra, equipado com um conjunto de operações sobre A.

Exemplo 1.1 Semigrupos, monóides, grupos e anéis são álgebras. As operações são as seguintes:

- Semigrupos têm apenas uma operação (binária);
- Monóides têm uma operação binária e uma constante (o elemento neutro);
- Grupos têm uma operação binária, uma constante e uma operação unária (inverso);
- Anéis têm as operações correspondentes à estrutura de grupo (zero, adição e elemento simétrico) e ainda uma outra operação binária (multiplicação); os anéis com unidade têm ainda uma outra constante (o elemento neutro da multiplicação).

Obviamente, um corpo é também uma álgebra (em particular é um anel), mas aquilo que distingue um corpo dum anel não tem carácter algébrico, pois consiste numa operação (inverso) que não está definida em todo o anel.

Exercício 1.2 O conjunto dos números naturais munido das operações de sucessor e predecessor forma uma álgebra?

2 Assinaturas e Σ-álgebras

Uma *assinatura* Σ consiste numa família $(\Sigma_n)_{n\in\mathbb{N}_0}$ de conjuntos disjuntos dois a dois. Usaremos também o símbolo Σ para denotar a união $\bigcup_{n\in\mathbb{N}_0} \Sigma_n$. Cada elemento de Σ_n é dito um *símbolo de operação de aridade* n, ou *símbolo de operação* n*-ário*. Para n igual a 0, 1, 2 e 3 os símbolos de operação são ditos, respectivamente, *símbolos de constante*, *unários*, *binários* e *ternários*.

Também se pode dizer *tipo de similaridade* em vez de assinatura, ou *tipo operacional*.

Seja Σ uma assinatura. Uma Σ-*álgebra* é um conjunto A equipado, para cada $f \in \Sigma_n$, com uma operação $f_A : A^n \to A$.

Exemplo 2.1 Seja Σ uma assinatura com os seguintes símbolos: $\mathbf{0}$ e $\mathbf{1}$ (0-ários), $\mathbf{s}$ (unário), $\mathbf{a}$ e $\mathbf{m}$ (binários). Qualquer anel, com a correspondência

$$\begin{aligned} \mathbf{0}_A &= 0 \, , \\ \mathbf{1}_A &= 1 \, , \\ \mathbf{a}_A &= + \, , \\ \mathbf{m}_A &= \cdot \, , \end{aligned}$$

é uma Σ-álgebra.

3 Homomorfismos

Sejam A e B duas Σ-álgebras. Um *homomorfismo* $h : A \to B$ é uma função que "preserva"as operações, i.e., tal que, para qualquer $f \in \Sigma_n$ e $x_1, \ldots, x_n \in A$,

$$h(f_A(x_1, \ldots, x_n)) = f_B(h(x_1), \ldots, h(x_n)) \, .$$

Um *isomorfismo* $i : A \to B$ é um homomorfismo bijectivo (cujo inverso é portanto também um homomorfismo).

Exemplo 3.1 Sejam A e B dois anéis. Uma função $h : A \to B$ é um homomorfismo de anéis se e só se é um homomorfismo de A e B vistos como álgebras para a assinatura Σ do Exemplo 2.1.

4 Congruências

Seja A uma Σ-álgebra. Uma relação de equivalência $\equiv$ sobre A diz-se uma relação de *congruência* (relativa a Σ) se para qualquer $f \in \Sigma_n$ e quaisquer $x_1, \ldots, x_n, y_1, \ldots, y_n \in A$,

$$((x_1 \equiv y_1) \wedge \ldots \wedge (x_n \equiv y_n)) \Rightarrow (f_A(x_1, \ldots, x_n) \equiv f_A(y_1, \ldots, y_n)) \, .$$

Se $\equiv$ é uma relação de congruência e $f \in \Sigma_n$ podemos definir uma função

$$f_{A/\equiv} : (A/\equiv)^n \to A/\equiv \, ,$$

para qualquer $x_1, \ldots, x_n \in A$, como

$$f_{A/\equiv}([x_1], \cdots, [x_n]) = [f_A(x_1, \ldots, x_n)] \, , \tag{1}$$

onde $[x]$ é a classe de equivalência de x, neste caso designada por *classe de congruência*. O conjunto quociente $A/\equiv$ equipado com todas as funções $f_{A/\equiv}$ assim definidas é a *álgebra quociente* de A por $\equiv$.

Exercício 4.1 Verifique que $f_{A/\equiv}$ é de facto uma função. (Na verdade uma relação de equivalência é de congruência se e só se para todos os símbolos de operação f a função $f_{A/\equiv}$ está bem definida — verifique.)

Teorema 4.2 *Seja A uma Σ-álgebra e $\equiv$ uma congruência sobre A. Para qualquer homomorfismo $h : A \to B$, com a propriedade de que $h(x) = h(y)$ sempre que $x \equiv y$, existe um e um só homomorfismo*

$$h^\sharp : A/\!\equiv\; \to B$$

tal que para qualquer $[x] \in A/\!\equiv$ se tem $h^\sharp([x]) = h(x)$.

Esta situação é representada pelo seguinte diagrama:

$$\begin{tikzcd} A \arrow[r, "{[\cdot]}"] \arrow[dr, "h"'] & A/\!\equiv \arrow[d, dotted, "h^\sharp"] \\ & B \end{tikzcd}$$

Proof. Seja B uma Σ-álgebra e $h : A \to B$ um homomorfismo. Seja

$$h^\sharp : A/\!\equiv\; \to B$$

a função definida pela condição

$$h^\sharp([x]) \stackrel{\text{def}}{=} h(x)\ .$$

A função está bem definida porque se $[x] = [y]$, ou seja, $x \equiv y$, tem-se por hipótese $h(x) = h(y)$. Além disso, $h^\sharp$ é claramente a única função que satisfaz a condição, uma vez que a condição define a função em todo o seu domínio. Seja agora $f \in \Sigma_n$ e $x_1, \ldots, x_n \in A$. Tem-se

$$\begin{array}{rcll} h^\sharp(f_{A/\equiv}([x_1], \ldots, [x_n]) & = & h^\sharp([f_A(x_1, \ldots, x_n)]) & \text{(Pela Def. de } f_{A/\equiv}) \\ & = & h(f_A(x_1, \ldots, x_n) & \text{(Por hipótese)} \\ & = & f_B(h(x_1), \ldots, h(x_n)) & \text{(Porque } h \text{ é um} \\ & & & \text{homomorfismo)} \\ & = & f_B(h^\sharp([x_1], \ldots, [x_n])) & \text{(Por hipótese)}\ . \end{array}$$

Portanto $h^\sharp$ é um homomorfismo $A \to B$. ∎

Teorema 4.3 *Seja A uma álgebra. O conjunto de todas as congruências sobre A é um reticulado completo onde os ínfimos são as intersecções em $\wp(A \times A)$.*

Proof. É simples ver que $A \times A$ é uma relação de congruência e que se $(\equiv_i)_i$ for uma família de relações de congruência também o é a intersecção $\bigcap_i \equiv_i$. Isto significa que o conjunto das congruências sobre A forma uma família de intersecção e portanto é um reticulado completo. ∎

O reticulado completo das congruências de A será denotado por $\mathrm{Cong}(A)$.

Seja A uma álgebra e ρ uma relação binária sobre A. A *congruência gerada* por ρ é a menor relação de congruência $\equiv_\rho$ que contém ρ; isto é, para a qual $x\rho y \Rightarrow x \equiv_\rho y$. Pelo teorema anterior, e devido à a equivalência entre famílias de intersecção e operadores de fecho, uma tal congruência de facto existe e é dada explicitamente por

$$\equiv_\rho \stackrel{\mathrm{def}}{=} \bigcap \{\equiv \in \mathrm{Cong}(A) \mid \rho \subseteq \equiv\} .$$

5 Núcleos de homomorfismos

A relação fundamental entre congruências e homomorfismos é expressa pelo seguinte resultado.

Teorema 5.1 *Seja A uma Σ-álgebra. Uma relação binária $\equiv$ sobre A é uma relação de congruência se e só se existe uma Σ-álgebra B e um homomorfismo $h : A \to B$ tal que*

$$x \equiv y \iff h(x) = h(y)$$

para qualquer $x, y \in A$.

Proof. Seja $\equiv$ uma congruência sobre A. Então $A/\equiv$ é uma Σ-álgebra, e a função $[\cdot] : A \to A/\equiv$ que a cada $x \in A$ faz corresponder a classe de congruência $[x]$ é um homomorfismo: seja $f \in \Sigma_n$; pelas equações (1) e (**??**) tem-se

$$[f_A(x_1, \ldots, x_n)] = f_{A/\equiv}([x_1], \ldots, [x_n]) .$$

Além disso tem-se $x \equiv y \iff [x] = [y]$, o que prova a existência dum homomorfismo nas condições pretendidas.

Agora seja $h : A \to B$ um homomorfismo de Σ-álgebras. Defina-se a relação binária $\equiv$ sobre A dada por $x \equiv y$ se $h(x) = h(y)$. É simples provar que esta relação é de equivalência. Além disso é de congruência: seja $f \in \Sigma_n$ e suponha-se $x_i \equiv y_i$ $(1 \leq i \leq n)$ em A. Então

$$h(f_A(x_1, \ldots, x_n)) = f_B(h(x_1), \ldots, h(x_n)) =$$

$$f_B(h(y_1), \ldots, h(y_n)) = h(f_A(y_1, \ldots, y_n)) ,$$

ou seja, $f_A(x_1, \ldots, x_n) \equiv f_A(y_1, \ldots, y_n)$. ∎

Dado um homomorfismo $h : A \to B$, a relação de congruência associada a h da forma descrita neste teorema é designada por *núcleo* de h e denota-se por $\ker h$.

Teorema 5.2 ("Primeiro teorema do isomorfismo".) *Sejam A e B Σ-álgebras e $h : A \to B$ um homomorfismo sobrejectivo. Então $A/\ker h \cong B$.*

Proof. Do teorema 4.2 sabemos que existe um e um só homomorfismo

$$k : A/\ker h \to B$$

tal que $k([a]) = h(a)$ para qualquer $a \in A$ e k é sobrejectivo porque h é. Por outro lado, se $k([a]) = k([b])$ então $h(a) = h(b)$, ou seja, $a \equiv b \bmod \ker h$, ou seja, $[a] = [b]$ em $A/\ker h$. portanto k é injectivo, sendo portanto um isomorfismo. ∎

Corolário 5.3 *Seja $h : A \to B$ um homomorfismo de Σ-álgebras. Então $A/\ker h \cong h(A)$.*

Corolário 5.4 *Um homomorfismo $h : A \to B$ de Σ-álgebras é injectivo se e só se $\ker h$ é a menor congruência sobre A (i.e., a relação de igualdade, ou diagonal, Δ_A).*

Teorema 5.5 *Seja A uma Σ-álgebra e $\rho \subseteq A \times A$ uma relação binária sobre A. Para qualquer homomorfismo $h : A \to B$ com a propriedade de que $h(x) = h(y)$ sempre que $x\rho y$ existe um e um só homomorfismo*

$$h^\sharp : A/{\equiv_\rho} \to B$$

tal que para qualquer $[x] \in A/{\equiv_\rho}$ se tem $h^\sharp([x]) = h(x)$.

Proof. Seja $h : A \to B$ um homomorfismo tal que $x\rho y \Rightarrow h(x) = h(y)$. Tem-se $\rho \subseteq \ker h$, e portanto $\equiv_\rho \subseteq \ker h$, pois $\equiv_\rho$ é por definição a menor congruência que contém ρ. O resultado pretendido obtém-se por aplicação do teorema 4.2. ∎

6 Σ-álgebras iniciais

Seja Σ uma assinatura. Um *termo* sobre Σ (abrev. Σ-termo) é um elemento do conjunto T_Σ definido recursivamente como se segue:

1. $\Sigma_0 \subseteq T_\Sigma$;
2. sejam $t_1, \ldots, t_n$ Σ-termos e $f \in \Sigma_n$; então $ft_1 \cdots t_n \in T_\Sigma$.

Os Σ-termos são portanto sempre *listas* de símbolos de operação.

Cada $f \in \Sigma_n$ define uma operação n-ária sobre T_Σ, dada por

$$f_{T_\Sigma}(t_1, \ldots, t_n) = ft_1 \cdots t_n ,$$

e portanto T_Σ tem também a estrutura duma Σ-álgebra, designada por *álgebra dos termos* (sobre Σ).

Teorema 6.1 *Seja Σ uma assinatura e A uma Σ-álgebra. Então existe um e um só homomorfismo $h : T_\Sigma \to A$.*

Proof. Ser um homomorfismo significa que, para quaisquer n Σ-termos t_1, $\ldots$, t_n e qualquer $f \in \Sigma_n$, h deve satisfazer a condição

$$h(f_{T_\Sigma}(t_1, \ldots, t_n) = f_A(h(t_1), \ldots, h(t_n)) ,$$

ou, equivalentemente,

$$h(ft_1 \ldots t_n) = f_A(h(t_1), \ldots, h(t_n)) .$$

Esta última condição é uma definição recursiva de h: se $n = 0$ então f é um símbolo de constante e $h(f) = f_A$; e a função h de facto existe e é única porque o valor $h(ft_1 \ldots t_n)$ é definido à custa de valores de h em Σ-termos cujo comprimento é estritamente inferior ao de $ft_1 \ldots t_n$. ∎

Escreveremos habitualmente t_A para o valor $h(t)$ dum termo em A, generalizando a notação utilizada para símbolos de constante.

Esta propriedade leva a que T_Σ seja também conhecida por Σ-álgebra *inicial*, uma terminologia que vem da teoria das categorias.

7 Geradores

Seja Σ uma assinatura e G um conjunto. Um *termo sobre Σ e G*, ou *Σ-termo sobre G*, é um elemento do conjunto $T_\Sigma(G)$, definido recursivamente como se segue:

1. $G \subseteq T_\Sigma(G)$;

2. $\Sigma_0 \subseteq T_\Sigma(G)$;

3. sejam $t_1, \ldots, t_n$ Σ-termos e $f \in \Sigma_n$; então $ft_1 \cdots t_n \in T_\Sigma(G)$.

Os Σ-termos sobre G são portanto sempre listas de símbolos de operação e elementos de G. O conjunto G permite "gerar" mais termos e os seus elementos são designados por *geradores* (de $T_\Sigma(G)$).

Exemplo 7.1 Sejam Σ a assinatura que apenas tem o símbolo de operação s (unário), e seja Σ' a assinatura que além deste tem também o símbolo 0 (constante). Tem-se $T_\Sigma = \emptyset$ e $T_\Sigma(\{0\}) = T_{\Sigma'} = \{0, s0, ss0, \ldots\}$.

Dada uma assinatura Σ e um conjunto G, o conjunto $T_\Sigma(G)$ tem, tal como T_Σ, uma estrutura de Σ-álgebra, onde para cada $f \in \Sigma_n$ e termos $t_1, \ldots t_n$ se tem

$$f_{T_\Sigma(G)}(t_1, \ldots, t_n) \stackrel{\mathrm{def}}{=} ft_1 \ldots t_n .$$

Esta álgebra designa-se por *Σ-álgebra livremente gerada por G*.

Teorema 7.2 *Seja Σ uma assinatura, G um conjunto e A uma Σ-álgebra. Então, para cada função $f : G \to A$ existe um e um só homomorfismo $f^\sharp : T_\Sigma(G) \to A$ tal que $f^\sharp(g) = f(g)$ para todos os geradores g.*

Dizemos habitualmente que $f^\sharp$ é o único homomorfismo que *estende* f, chamamos a $f^\sharp$ a *extensão homomórfica* de f, e representamos esta situação por meio do diagrama seguinte:

$$\begin{tikzcd} G \arrow[r, "\subseteq"] \arrow[dr, "f"'] & T_\Sigma(G) \arrow[d, dotted, "f^\sharp"] \\ & A \end{tikzcd}$$

Proof. Semelhante à prova do Teorema 6.1. Agora a base da definição recursiva tem duas partes: a dos símbolos de contante, como antes, e a dos geradores. ∎

Dada uma função $f : G \to A$ como acima, escreveremos habitualmente t_f para o valor $f^\sharp(t)$ dum termo t.

Exemplo 7.3 Considere a assinatura Σ do exemplo anterior, e seja $f : \{0\} \to \mathbb{N}$ uma função, onde $\mathbb{N}$ é o conjunto dos números naturais equipado com a operação de *sucessor* ($n \mapsto n + 1$). Uma vez fixado o valor $f(0)$, a qualquer termo é atribuído um valor único pela extensão homomórfica de f. Por exemplo, se $f(0) = 100$ ter-se-á $f(s0) = 101$, $f(ss0) = 102$, etc.

8 Variáveis de equações

Usualmente não trabalhamos com álgebras livres como acima. Por exemplo, a álgebra inicial correspondente a uma assinatura de álgebra de Boole não é uma álgebra de Boole, pois não satisfaz as propriedades algébricas que relacionam as várias operações. Por exemplo, as fórmulas 1 e $(1 \wedge 1)$ correspondem a termos distintos, enquanto que numa álgebra de Boole deveríamos ter $1 = 1 \wedge 1$. Isto não significa que não exista uma álgebra de Boole, i.e., uma álgebra de Boole a partir da qual existe um e um só homomorfismo de álgebras de Boole para qualquer outra álgebra de Boole: a álgebra de Boole $2 = \{0, 1\}$ com $0 \leq 1$ é inicial (verifique). O nosso objectivo agora é tratar álgebras que obedecem a leis tais como a associatividade da operação $\wedge$, etc., que é expressa por meio de variáveis como:

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z \ .$$

Seja então Σ uma assinatura e X um conjunto, cujos elementos designaremos por *variáveis*. [Assumiremos sempre que o conjunto de variáveis é disjunto do conjunto de símbolos de operação da assinatura.] Uma Σ-*equação* sobre X, ou *lei algébrica* sobre X, é um par (t, u) de termos de $T_\Sigma(X)$. Uma equação (t, u) é geralmente escrita na forma "$t = u$".

9 (Σ, E)-álgebras

Seja agora A uma Σ-álgebra. Dizemos que a álgebra A *satisfaz* uma equação $t = u$ sobre X, e escrevemos $A \models t = u$, se para qualquer função $f : X \to A$ se tem $t_f = u_f$. Intuitivamente, $A \models t = u$ diz-nos que a equação é verdadeira independentemente dos valores de A que "atribuirmos" às variáveis.

Dada a propriedade universal de $T_\Sigma(X)$, a condição $A \models t = u$ pode ser formulada equivalentemente da seguinte forma:

Proposição 9.1 *$A \models t = u$ se e só se $h(t) = h(u)$ para qualquer homomorfismo $h : T_\Sigma(X) \to A$.*

Uma *especificação algébrica* sobre um conjunto X de variáveis é um par (Σ, E), onde Σ é uma assinatura e E é um conjunto (finito ou infinito) de Σ-equações sobre X. Uma Σ-álgebra A *satisfaz* a especificação (Σ, E), e escrevemos $A \models E$, se satisfaz todas as suas equações.

10 (Σ, E)-congruências

Seja (Σ, E) uma especificação algébrica e $\equiv$ uma congruência sobre uma Σ-álgebra A. Dizemos que $\equiv$ *satisfaz* a especificação se $A/{\equiv}$ satisfaz a especificação.

Teorema 10.1 *As congruências de A que satisfazem (Σ, E) formam uma família de intersecção:*

- *$A \times A$ satisfaz (Σ, E);*
- *Se todas as congruências $\equiv_i$ duma família não vazia $(\equiv_i)_{i \in I}$ satisfazem (Σ, E) então a intersecção $\bigcap_{i \in I} \equiv_i$ satisfaz (Σ, E).*

Proof. É evidente que $A \times A$ satisfaz a especificação. Seja então $(\equiv_i)_i i \in I$ uma família não vazia de congruências que satisfazem a especificação. Para cada $i \in I$ existe um e um só homomorfismo $q'_i : A/{\equiv} \to A/{\equiv_i}$ que comuta com os quocientes $q : A \to A/{\equiv}$ e $q_i : A \to A/{\equiv_i}$,

$$\begin{tikzcd} A \arrow[r, "q"] \arrow[dr, "q_i"'] & A/{\equiv} \arrow[d, "q'_i"] \\ & A/{\equiv_i} \end{tikzcd}$$

onde escrevemos $\equiv$ em vez de $\bigcap_{i \in I} \equiv_i$; isto resulta de $\equiv \subseteq \equiv_i$ e do Teorema 4.2.

Sejam $a, b \in A$. Tem-se $q(a) = q(b)$ em $A/{\equiv}$ se e só se $a \equiv b$, se e só se $a \equiv_i b$ para qualquer $i \in I$, se e só se para qualquer $i \in I$ se tem

$q_i(a) = q_i(b)$, se e só se $q'_i(q(a)) = q'_i(q(b))$ para qualquer $i \in I$. Por outras palavras, $\bigcap_{i \in I} \ker q'_i = \Delta_{A/\equiv}$, ou seja, para quaisquer $x, y \in A/\equiv$ tem-se $x = y$ se e só se $q'_i(x) = q'_i(y)$ para qualquer $i \in I$.

Seja agora $t = u$ uma equação arbitrária de E, satisfeita por todas as congruências $\equiv_i$, e seja $h : T_\Sigma(X) \to A/\equiv$ um homomorfismo. Para qualquer $i \in I$ tem-se, por hipótese, $q'_i(h(t)) = q'_i(h(u))$ em $A/\equiv_i$, e portanto pelo que acabámos de ver tem-se $h(t) = h(u)$. Logo, $A/\equiv \models t = u$. ∎

Corolário 10.2 *Seja A uma Σ-álgebra e (Σ, E) uma especificação algébrica. Então existe a menor congruência $\equiv$ sobre A que satisfaz E. A álgebra $A/\equiv$ tem a propriedade de que qualquer homomorfismo $h : A \to B$ para uma (Σ, E)-álgebra B se factoriza duma forma única através do quociente $A \to A/\equiv$.*

Exemplo 10.3

1. Seja M um monóide. Então existe a menor conguência $\equiv$ de monóides sobre M tal $M/\equiv$ é um monóide comutativo. Qualquer homomorfismo de monóides $h : M \to N$ em que N é comutativo tem uma factorização única através do quociente $M \to M/\equiv$. Portanto há uma bijecção entre o conjunto dos homomorfismos de monóides $M \to N$ com N comutativo e o conjunto dos homomorfismos de monóides $M/\equiv \to N$.

2. Seja Φ o conjunto das fórmulas do cálculo proposicional, identificado com $T_\Sigma(\Pi)$, onde Π é o conjunto dos símbolos proposicionais e Σ é a assinatura das álgebras de Boole:

$$\Sigma_0 = \{0, 1\}, \qquad \Sigma_1 = \{\neg\}, \qquad \Sigma_2 = \{\wedge, \vee, \to\}$$

(e $\Sigma_n = \emptyset$ para $n \geq 3$). Sendo $\equiv$ a menor congruência que torna Φ uma álgebra de Boole, o quociente $\Phi/\equiv$ é precisamente a álgebra de Lindenbaum $\mathcal{L}$ do cálculo proposicional. Tem-se portanto que para qualquer álgebra de Boole B e qualquer função $f : \Pi \to B$ existe um e um só homomorfismo de álgebras de Boole

$$h : \mathcal{L} \to B$$

tal que $h([P_i]) = f(P_i)$ para cada símbolo proposicional. No caso $B = 2$ obtém-se a propriedade conhecida das valorações. O conteúdo do teorema da adequação do cálculo proposicional é precisamente que $\equiv$ coincide com a intersecção dos núcleos de todas as valorações $v : \Phi \to 2$.

11 (Σ, E)-álgebras iniciais

Seja (Σ, E) uma especificação algébrica. Denotando por $\equiv$ a menor congruência sobre T_Σ que satisfaz E, denotaremos por $T_{(\Sigma,E)}$ o quociente $T_\Sigma/\equiv$. Esta é a (Σ, E)-*álgebra inicial*, no sentido seguinte:

Teorema 11.1 *Seja* (Σ, E) *uma especificação algébrica e* A *uma* (Σ, E)*-álgebra. Então existe um e um só homomorfismo* $h : T_{(\Sigma,E)} \to A$.

Proof. Já sabemos que existe um e um só homomorfismo $h : T_\Sigma \to A$, ao qual corresponde portanto um homomorfismo $T_{(\Sigma,E)} \to A$, que é único devido à unicidade de h. ∎

Exemplo 11.2 1. Seja Σ a assinatura com símbolos "0" e "1" (constantes), "$-$" (unário), e "+" e "$\cdot$" (binários). Sejam x e y variáveis, e seja E o conjunto com as equações seguintes, onde escrevemos "xy" em vez de "$\cdot xy$", "$xy + z$" em vez de "$+ \cdot xyz$", etc.

$$\begin{aligned}
x + (y + z) &= (x + y) + z \\
x + y &= y + x \\
x + 0 &= x \\
x + (-x) &= 0 \\
x(yz) &= (xy)z \\
x1 &= x \\
1x &= x \\
x(y + z) &= xy + xz \\
(x + y)z &= xz + yz
\end{aligned}$$

Uma (Σ, E)-álgebra é um anel (com unidade). A álgebra inicial $T_{(\Sigma,E)}$ é o anel $\mathbf{Z}$ dos números inteiros.

2. 2 é uma álgebra de Boole inicial.

12 (Σ, E)-álgebras livres

De modo análogo se obtém a (Σ, E)-álgebra gerada por um conjunto de geradores G, que denotamos por $T_{(\Sigma,E)}(G)$: é o quociente da álgebra livre $T_\Sigma(G)$ pela menor congruência sobre $T_\Sigma(G)$ que satisfaz as equações de E. Tudo é semelhante ao que foi visto na secção anterior para a (Σ, E)-álgebra inicial e os pormenores deixam-se como exercício. A propriedade universal que caracteriza estas álgebras livres é expressa pelo seguinte teorema:

Teorema 12.1 *Seja* (Σ, E) *uma especificação algébrica (sobre um conjunto de variáveis* X*) e* G *um conjunto (de geradores) disjunto de* X *e de* Σ*. Então, dada qualquer função*

$$f : G \to A \;,$$

onde A *é uma* (Σ, E)*-álgebra, existe um e um só homomorfismo*

$$f^\sharp : T_{(\Sigma,E)}(G) \to A$$

tal que $f^\sharp([g] = f(g)$ para qualquer gerador g. Esta situação é expressa pelo diagrama seguinte:

$$\begin{tikzcd} G \arrow[r, "{[\cdot]}"] \arrow[dr, "f"'] & T_{(\Sigma,E)}(G) \arrow[d, dotted, "f^\sharp"] \\ & A \end{tikzcd}$$

Dado um elemento $a \in T_{(\Sigma,E)}(G)$, denotaremos habitualmente por a_f o valor $f^\sharp(a)$, generalizando assim a notação introduzida na secção 7. A função que a cada gerador g atribui $[g]$ é designada por *injecção de geradores*.

13 Geradores e relações

Seja (Σ, E) uma especificação algébrica e G um conjunto (de "geradores"). Uma *relação de definição* (de (Σ, E)-álgebras) sobre G é um par (a, b), onde $a, b \in T_{(\Sigma,E)}(G)$, usualmente escrito como uma equação "$a = b''$.

Seja agora A uma (Σ, E)-álgebra e seja $f : G \to A$ uma função. Dizemos que a relação de definição $a = b$ é *respeitada* por f se $a_f = b_f$. Do mesmo modo, se ρ é um conjunto de relações, dizemos que f respeita ρ se respeita todas as relações de ρ.

Um conjunto de relações ρ equivale a uma relação binária sobre $T_{(\Sigma,E)}(G)$, o que nos permite falar da congruência gerada por ρ. A álgebra quociente $T_{(\Sigma,E)}(G)/{\equiv_\rho}$ é designada por álgebra *apresentada por G e ρ*, e denotamo-la por $T_{(\Sigma,E)}(G \mid \rho)$. A função que a cada gerador g faz corresponder a classe de equivalência $[g]$ é designada por *injecção de geradores*, ou *inclusão de geradores*.

Teorema 13.1 *Seja (Σ, E) uma especificação algébrica, G um conjunto, ρ um conjunto de relações em $T_{(\Sigma,E)}(G)$, e A uma (Σ, E)-álgebra. Então, para cada função $f : G \to A$ que respeita as relações existe um e um só homomorfismo $h : T_{(\Sigma,E)}(G \mid \rho) \to A$ tal que $h([g]) = f(g)$ para todos os geradores g.*

Esta situação é representada pelo seguinte diagrama:

$$\begin{tikzcd} G \arrow[r, "{[\cdot]}"] \arrow[dr, "f"'] & T_{(\Sigma,E)}(G \mid \rho) \arrow[d, dotted, "h"] \\ & A \end{tikzcd}$$

Proof. Nesta prova será útil usar nomes explícitos para as várias funções e homomorfismos que vão surgindo. Por exemplo, chamaremos η à função que a cada gerador $g \in G$ atribui a classe de equivalência $[g] \in T_\Sigma(G \mid \rho)$:

$$\begin{tikzcd} G \arrow[r, "\eta"] \arrow[dr, "f"'] & T_{(\Sigma,E)}(G \mid \rho) \arrow[d, dotted, "h"] \\ & A \end{tikzcd}$$

O enunciado do teorema pode portanto ser reformulado equivalentemente dizendo que para cada função $f : G \to A$ que respeita as relações existe um e um só homomorfismo $h : T_\Sigma(G \mid \rho) \to A$ tal que $h \circ \eta = f$.

Seja $\iota : G \to T_{(\Sigma,E)}(G)$ a injecção de geradores de G em $T_{(\Sigma,E)}(G)$. Pelo Teorema 12.1 existe um e um só homomorfismo

$$\eta^\sharp : T_{(\Sigma,E)}(G) \to T_{(\Sigma,E)}(G \mid \rho)$$

tal que $\eta = \eta^\sharp \circ \iota$. Seja agora A uma (Σ, E)-álgebra arbitrária e $f : G \to A$ uma função. Novamente pelo Teorema 12.1, existe um homomorfismo único $f^\sharp : T_{(\Sigma,E)}(G) \to A$ tal que $f = f^\sharp \circ \iota$. As várias funções e homomorfismos descritos até este momento estão representados no seguinte diagrama:

$$\begin{tikzcd} G \arrow[rr, "\eta"] \arrow[dr, "\iota"] \arrow[ddr, "f"'] & & T_{(\Sigma,E)}(G \mid \rho) \\ & T_{(\Sigma,E)}(G) \arrow[ur, "\eta^\sharp"] \arrow[d, "f^\sharp"] & \\ & A & \end{tikzcd}$$

Seja agora $h : T_{(\Sigma,E)}(G \mid \rho) \to A$ um homomorfismo qualquer. Se $h \circ \eta^\sharp = f^\sharp$ então $h \circ \eta = f$, pois

$$h \circ \eta = h \circ \eta^\sharp \circ \iota = f^\sharp \circ \iota = f \ .$$

Por outro lado, $h \circ \eta = f$ é equivalente a $h \circ \eta^\sharp \circ \iota = f$. Mas $f^\sharp$ é o único homomorfismo tal que $f^\sharp \circ \iota = f$, e portanto tem de ter-se $h \circ \eta^\sharp = f^\sharp$. Acabámos portanto de ver que dado um homomorfismo $h : T_{(\Sigma,E)}(G \mid \rho) \to A$ as condições $h \circ \eta = f$ e $h \circ \eta^\sharp = f^\sharp$ são equivalentes.

Finalmente, dizer que f respeita uma relação $a = b$ significa que $a_f = b_f$, ou seja, $f^\sharp(a) = f^\sharp(b)$. Pelo teorema 5.5 resulta então que existe um e um só homomorfismo $h : T_{(\Sigma,E)}(G \mid \rho) \to A$ tal que $h \circ \eta^\sharp = f^\sharp$, ou seja, equivalentemente, tal que $h \circ \eta = f$. ∎

Exemplo 13.2 Considere-se uma fórmula φ do cálculo proposicional. Denotanto por $[\varphi]$ a classe de equivalência de φ na álgebra de Lindenbaum $\mathcal{L}$, a álgebra de Boole B apresentada pelos símbolos proposicionais e pela relação $[\varphi] = 1$ tem a propriedade de que para qualquer outra fórmula ψ se tem $[\psi] = 1$ em B se e só se $\varphi \vdash \psi$. Por outras palavras, o quociente B de $\mathcal{L}$ corresponde à *teoria* obtida tomando como axioma adicional a fórmula φ. Isto é geral: a teoria gerada por um conjunto de fórmulas Ψ do cálculo proposicional coincide com o conjunto de fórmulas que são iguais a 1 no quociente de $\mathcal{L}$ pela menor congruência $\equiv$ sobre $\mathcal{L}$ que satisfaz $[\psi] \equiv 1$ para todas as fórmulas $\psi \in \Psi$.

Exemplo 13.3 Sejam A e B (Σ, E)-álgebras. Tomemos como conjunto de geradores a união disjunta $G = A \amalg B$ e denote-se a álgebra livre $T_{(\Sigma,E)}(G)$ por $\mathfrak{L}$. Considere-se como relações de definição as condições

$$\begin{aligned} [f_A(a_1, \ldots, a_n)] &= f_{\mathfrak{L}}([a_1], \ldots, [a_n]) \\ [f_B(b_1, \ldots, b_n)] &= f_{\mathfrak{L}}([b_1], \ldots, [b_n]) \ , \end{aligned}$$

onde f é um símbolo n-ário arbitrário e $a_1, \ldots, a_n \in A$ e $b_1, \ldots, b_n \in B$ são elementos arbitrários das álgebras A e B. Dada uma álgebra arbitrária C, uma função $f : G \to C$ é o mesmo que um par de funções $f_1 : A \to C$ e $f_2 : B \to C$ (uma vez que G é a união disjunta de A e B) e o significado das relações de definição é o seguinte: a função f respeita as relações se e só se f_1 e f_2 forem homomorfismos. Por outras palavras, uma função $f : G \to C$ que respeita as relações é "o mesmo" que um par de homomorfismos $f_1 : A \to C$ e $f_2 : B \to C$. Posto isto é fácil concluir que a álgebra apresentada por G e pelas relações é o *coproduto* de A e B, que denotaremos por $A + B$: dado um qualquer par de homomorfismos $h : A \to C$ e $k : B \to C$ existe um e um só homomorfismo $[h, k] : A + B \to C$ tal que

$$\begin{aligned} [h, k] \circ i &= h \\ [h, k] \circ j &= k \ , \end{aligned}$$

onde $i : A \to A+B$ e $j : B \to A+B$ são os homomorfismos correspondentes à injecção de geradores $G \to A+B$. Da mesma forma se constrói o coproduto de qualquer família $(A_i)_{i \in I}$ de (Σ, E)-álgebras indexada por um conjunto I.

14 Álgebras heterogéneas

As álgebras heterogéneas, ou multi-género, consistem numa generalização das álgebras vistas até aqui na qual existem elementos de *géneros* diferentes. Por exemplo, num espaço vectorial real V cada número real λ é identificado com uma operação unária sobre V (multiplicação por λ), mas também é possível encarar conjuntamente $\mathbb{R}$ e V como uma única álgebra munida duma operação binária de multiplicação por escalar

$$\mathbb{R} \times V \to V \ .$$

As diferenças são as seguintes. Começamos por assumir a existência dum conjunto S de *géneros* (e.g., o género dos números reais e o género dos vectores, no exemplo anterior) e por *assinatura* Σ entendemos agora uma família $(\Sigma_i)_{i\in S^*\times S}$ de conjuntos (de símbolos de operação) disjuntos dois a dois.

Cada símbolo $f \in \Sigma_{(w,s)}$ é agora pensado como uma função com argumentos $w_1, \ldots, w_n$, onde $n = |w|$, e que tem valores do género s.

Uma Σ-álgebra A é por isso definida como uma família $(A_s)_{s\in S}$ de conjuntos equipada, para cada $f \in \Sigma_{(w,s)}$, com uma operação (função)

$$f_A : A_{w_1} \times \ldots \times A_{w_{|w|}} \to A_s \; .$$

Um *homomorfismo* $h : A \to B$ é uma família $(h_s)_{s\in S}$ de funções $h_s : A_s \to B_s$ tal que para cada $f \in \Sigma_{(w,s)}$, $x_1 \in A_{w_1}, \ldots, x_{|w|} \in A_{w_{|w|}}$,

$$h_s(f_A(x_1, \ldots, x_{|w|}) = f_B(h_{w_1}(x_1), \ldots h_{w_{|w|}}(x_{|w|})) \; .$$

A noção de congruência passa a consistir de uma família de relações de equivalência, também indexada por S, satisfazendo as condições que neste momento já deverão ser óbvias para o leitor. Toda a teoria que foi exposta nestas folhas se generaliza da forma natural para o caso das álgebras heterogéneas. Exercício: enuncie e demonstre os teoremas correspondentes.

15 Alguns problemas

1. Seja (Σ, E) uma especificação algébrica e A e B Σ-álgebras. Definindo uma estrutura de Σ-álgebra no produto cartesiano $A \times B$ por

   $$f_{A\times B}((x_1, y_1), \ldots, (x_n, y_n)) = (f_A(x_1, \ldots, x_n), f_B(y_1, \ldots, y_n))$$

   para cada $f \in \Sigma_n$ e $x_i \in A$, $y_i \in B$, mostre que:

   (a) as projecções $\pi_1 : A \times B \to A$ e $\pi_2 : A \times B \to B$ são homomorfismos;

   (b) se A e B forem (Σ, E)-álgebras então $A \times B$ é uma (Σ, E)-álgebra.

2. Seja A uma Σ-álgebra e $(\equiv_i)_{i\in I}$ uma família de relações de congruência sobre A. Seja ainda $\equiv$ a intersecção $\bigcap_{i\in I} \equiv_i$.

   (a) Justifique que para cada i existe um homomorfismo

   $$q_i : A/{\equiv} \to A/{\equiv_i}$$

   tal que para cada $a \in A$ se tem $[a]_\equiv \mapsto [a]_{\equiv_i}$.

(b) Mostre que a intersecção

$$\bigcap_{i \in I} \ker q_i$$

é a relação diagonal sobre $A/\equiv$.

3. Um *morfismo de assinaturas* $\Sigma \to \Sigma'$ é uma família de funções $f_n : \Sigma_n \to \Sigma'_n$. A categoria das assinaturas resultante é portanto a categoria $\mathrm{Set}/\mathbb{N}$.

   (a) Mostre que se $f : \Sigma \to \Sigma'$ é um morfismo de assinaturas e A é uma Σ'-álgebra então A é uma Σ-álgebra, que denotamos por $f^*(A)$, ou $(A)_f$, e designamos por "reduto de A ao longo de f", ou "pullback de A ao longo de f".

   (b) A *categoria das álgebras sobre assinatura variável* é definida da seguinte forma:

      i. Objectos: pares (Σ, A) com A uma Σ-álgebra.

      ii. Setas: uma seta $f : (\Sigma, A) \to (\Sigma', A')$ é um par (g, h) onde $g : \Sigma \to \Sigma'$ é um morfismo de assinaturas e $h : A \to g^*(A')$ é um homomorfismo de Σ-álgebras.

   Mostre que estes dados definem de facto uma categoria.

4. Mostre que a atribuição $A \mapsto f^*(A)$ é parte dum functor da categoria das Σ'-álgebras para a categoria das Σ-álgebras.

5. Seja $f : \Sigma \to \Sigma'$ um morfismo de assinaturas e A uma Σ-álgebra.

   (a) Mostre que existe uma maneira natural de definir uma Σ'-álgebra $f_!(A)$ a partir de A, como um quociente apropriado de $T_{\Sigma'}(A)$, de tal forma que a injecção de geradores

   $$i : A \to f_!(A)$$

   seja um homomorfismo de Σ-álgebras quando $f_!(A)$ é visto como Σ-álgebra por pullback de $f_!(A)$ ao longo de f. Sugestão: considere a Σ'-álgebra apresentada por geradores e relações tomando A como conjunto de geradores e, para cada $\omega \in \Sigma_n$ e $a_1, \ldots a_n \in A$, a relação

   $$\omega_A(a_1, \ldots, a_n) = f(w)a_1 \ldots a_n \, .$$

   (b) Mostre que o homomorfismo $i : A \to f^*(f_!(A))$ assim definido tem a seguinte propriedade universal: para cada Σ'-álgebra B e cada homomorfismo de Σ-álgebras $h : A \to f^*(B)$ existe um e um só homomorfismo de Σ'-álgebras $h' : f_!(A) \to B$ tal que $h' \circ i = h$.

(c) Mostre que a propriedade universal acima é uma generalização da propriedade universal da inclusão $X \to T_{\Sigma'}(X)$, quando X é um conjunto qualquer (pense num conjunto como uma Σ-álgebra para $\Sigma = \emptyset$).

6. Considere a seguinte assinatura NAT com um único género nat e as operações

$$\begin{aligned} \text{zero} &: \ \to \text{nat} \\ \text{successor} &: \ \text{nat} \to \text{nat} \end{aligned}$$

   (a) Mostre que $\mathbb{N}_0$ é uma NAT-álgebra.
   (b) Mostre que $\mathbb{N}_0$ é isomorfa à álgebra inicial T_{NAT}.

7. Considere a especificação ADD com um único género nat e as seguintes operações e axiomas:

   - Operações:

$$\begin{aligned} \text{zero} &: \ \to \text{nat} \\ \text{successor} &: \ \text{nat} \to \text{nat} \\ \text{add} &: \ \text{nat nat} \to \text{nat} \end{aligned}$$

   - Axiomas:

$$\begin{aligned} \text{add}(\text{zero}, n) &= n \\ \text{add}(\text{successor}(m), n)) &= \text{successor}(\text{add}(m, n)) \end{aligned}$$

   (a) Mostre que $\mathbb{N}_0$ é uma ADD-álgebra.
   (b) Mostre que $\mathbb{N}_0$ é isomorfa à ADD-álgebra inicial.

8. Considere a seguinte especificação do tipo de dados pilha (stack) de números inteiros, cuja assinatura se designa por STACK e cujo conjunto de axiomas se designa por E.

   - Géneros: int, stack
   - Operações:

$$\begin{aligned} \text{new} &: \ \to \text{stack} \\ \text{push} &: \ \text{stack int} \to \text{stack} \\ \text{pop} &: \ \text{stack} \to \text{stack} \\ \text{top} &: \ \text{stack} \to \text{int} \end{aligned}$$

- Axiomas:

$$\begin{aligned}
\mathrm{pop}(\mathrm{push}(s,i)) &= s\\
\mathrm{top}(\mathrm{push}(s,i)) &= i\\
\mathrm{pop}(\mathrm{new}) &= \mathrm{new}\\
\mathrm{top}(\mathrm{new}) &= 0
\end{aligned}$$

Considere também a seguinte STACK-álgebra C:

- $C_{\mathrm{int}} = \mathbb{Z}$
- $C_{\mathrm{stack}} = \mathbb{Z}^{\mathbb{N}_0} \times \mathbb{N}_0$
- $\mathrm{new}_C = (\text{sucessão nula}, 0)$
- $\mathrm{push}_C((s_n), p, i) = ((t_n), p+1)$, onde

$$t_n = \begin{cases} i & \text{se } n = p+1 \\ s_n & \text{se } n \neq p+1 \end{cases}$$

- $\mathrm{pop}_C((s_n), p) = \begin{cases} ((s_n), p-1) & \text{se } p \neq 0 \\ ((s_n), p) & \text{se } p = 0 \end{cases}$
- $\mathrm{top}_C((s_n), p) = s_p$

(Para simplificar assuma que as operações do género int são todas constantes, i.e., 0, 1, -1, etc., sendo a interpretação em C feita da maneira natural: $0_C = 0 \in \mathbb{Z}$, etc.)

(a) Diga, justificando, se a STACK-álgebra C satisfaz os axiomas da especificação.

(b) Mostre que existe um homomorfismo

$$h : C \to T_{(\mathrm{STACK},E)}$$

que a cada elemento $((s_n), p) \in C_{\mathrm{stack}}$ faz corresponder a classe de equivalência de $\mathrm{push}(\mathrm{push}(\ldots(\mathrm{push}(\mathrm{new}, s_1), s_2), \ldots), s_p)$ na álgebra inicial (e tal que h_{int} é uma bijecção).

(c) Justifique que h_{stack} é sobrejectivo e conclua que existe uma congruência $\equiv$ sobre C tal que $C/\!\equiv$ é isomorfa à (STACK,E)-álgebra inicial.

(Isto significa que a álgebra C é uma implementação correcta da especificação.)

9. Considere a especificação do tipo de dados fila de espera de números inteiros com dois géneros int e queue, símbolos de operação

$$\begin{aligned}
\mathrm{new} &: \ \to \mathrm{queue}\\
\mathrm{enter} &: \ \mathrm{queue}\ \mathrm{int} \to \mathrm{queue}\\
\mathrm{exit} &: \ \mathrm{queue} \to \mathrm{queue}\\
\mathrm{first} &: \ \mathrm{queue} \to \mathrm{int}\ .
\end{aligned}$$

e axiomas

$$\begin{aligned}
\text{first}(\text{enter}(\text{new}, n)) &= n \\
\text{first}(\text{enter}(\text{enter}(q, m), n)) &= \text{first}(\text{enter}(q, m)) \\
\text{exit}(\text{enter}(\text{new}, n)) &= \text{new} \\
\text{exit}(\text{enter}(\text{enter}(q, m), n)) &= \text{exit}(\text{enter}(q, m)) \\
\text{first}(\text{new}) &= 0 \\
\text{exit}(\text{new}) &= \text{new}
\end{aligned}$$

(a) Considerando a assinatura QUEUE assim definida, defina uma QUEUE-álgebra C tal que

$$\begin{aligned}
C_{\text{int}} &= \mathbb{Z} \\
C_{\text{queue}} &= \mathbb{Z}^{\mathbb{N}_0} \times \mathbb{N}_0 \times \mathbb{N}_0 \\
\text{new}_C &= ((0)_{n \in \mathbb{Z}}, 0, 0)
\end{aligned}$$

(Sugestão: isto corresponde à implementação duma fila de espera por meio duma lista infinita e dois ponteiros. Para cada fila (a, p, q) os valores da fila são $a_p, \ldots, a_{q-1}$, sendo o primeiro valor (o que vai sair a seguir) o da posição p e o último o da posição $q - 1$.)

(b) Verifique que C satisfaz os axiomas, ou modifique a álgebra C por forma a que estes sejam satisfeitos.

(c) Mostre que existe um homomorfismo sobrejectivo de C para a (QUEUE, E)-álgebra inicial.