

Lecture 8 Corrected. Algebra, continued. Section 4: Word algebras and Freedom (Freeness).

0. Preliminary notes.....	1
1. Freedom for algebras. Word algebras, initial algebras.....	1
1.1. Word algebras.....	1
1.2. Word algebras and homomorphisms. Initial algebra.....	3
2. Word algebra on a set. Free algebra.....	4
2.1. Word algebra on a set.....	4
2.2. Homomorphisms from a word algebra on a set. Free algebra.....	5
Homework 8.2.....	6

No reading. Our handouts are mainly a compilation from the PtMW textbook and two other sources listed below. Algebra Section 4 (this lecture) is based on the last two.

Cohn P.M. Universal algebra, Harper and Row. New York, Evanston and London, 1965.

Burstall R.M. and J.A. Goguen, Algebras, Theories and Freeness: An Introduction for Computer Scientists. In: M. Broy and G. Schmidt (eds.) Theoretical Foundations of Programming Methodology, Reidel, 1982, pp. 329 – 349.

0. Preliminary notes.

Let us return to the algebras considered in Lecture 4 (7). We considered the homomorphism $f: \mathbf{Mod4} \rightarrow \mathbf{Mod2}$. Are there any homomorphisms from $\mathbf{Mod2}$ to $\mathbf{Mod4}$? We show that there are none. Suppose that $h: \mathbf{Mod2} \rightarrow \mathbf{Mod4}$ is such a homomorphism. Then, by definition of a homomorphism, $h(\mathbf{zero}_{\mathbf{Mod2}}) = \mathbf{zero}_{\mathbf{Mod4}}$, i.e. $h(0) = 0$, $h(\mathbf{one}_{\mathbf{Mod2}}) = \mathbf{one}_{\mathbf{Mod4}}$, i.e. $h(1) = 1$. So far it is OK. But by the same definition $h(\mathbf{one}_{\mathbf{Mod2}} + \mathbf{one}_{\mathbf{Mod2}})$ should be equal to $h(\mathbf{one}_{\mathbf{Mod2}}) + h(\mathbf{one}_{\mathbf{Mod2}}) = \mathbf{one}_{\mathbf{Mod4}} + \mathbf{one}_{\mathbf{Mod4}} = 2$. On the other hand, in $\mathbf{Mod2}$ we have $\mathbf{one}_{\mathbf{Mod2}} + \mathbf{one}_{\mathbf{Mod2}} = 0$ and $h(0) = 0$. So we have inconsistency $h(\mathbf{one}_{\mathbf{Mod2}} + \mathbf{one}_{\mathbf{Mod2}}) = 2$ and $h(\mathbf{one}_{\mathbf{Mod2}} + \mathbf{one}_{\mathbf{Mod2}}) = 0$, i.e., $h(0) = 0$ and $h(0) = 2$. So there is no homomorphism from $\mathbf{Mod2}$ to $\mathbf{Mod4}$.

One of the properties of these two algebras is that the same result can be obtained in many different ways. For example, in $\mathbf{Mod2}$ we have $1 + 1 = 0 + 0 = 0$. These algebras are not *free*: some nontrivial equalities hold in them. This is the reason why homomorphisms of one Ω -algebra into another are in some cases impossible. Below we will consider Ω -algebras which can be homomorphically mapped to any Ω -algebra.

1. Freedom for algebras. Word algebras, initial algebras.

1.1. Word algebras.

For any signature Ω there is a particularly interesting algebra called the *word algebra* which we denote as \mathbf{W}_Ω . Actually, we have considered word algebras when we have defined the syntax of Statement Logic (and Predicate Logic). Let us do it now using the algebraic terminology.

The elements of the word algebra (of its carrier) are “syntactical” expressions: they are words (strings) “built” from the symbols of the given signature as letters of the alphabet (with

addition brackets and sometimes other punctuation symbols). The basic expressions are the 0-ary symbols, strictly speaking they are one-letter words. And the operations produce larger expressions (larger words) from smaller ones using symbols of operations and brackets. Let us see what this means with an example.

But first of all note that there are several traditions for constructing such expressions: one is the more general *prefix* form which is suitable for operations of any arity, another is the *infix* form which is more traditional in arithmetic and logic for familiar binary operations. Illustration: “(3 + 5)” is in infix form; “+(3,5)” is in prefix form. In the arithmetic and logical examples below we will use infix form for binary operations.

Example. Let us consider the signature $\Omega_{\text{Numb}} = \{\mathbf{zero}, \mathbf{one}, +, \mathbf{X}\}$ and the word algebra $\mathbf{W}_{\Omega_{\text{Numb}}}$. Its carrier $W_{\Omega_{\text{Numb}}}$ consist of words formed by symbols of the signature Ω_{Numb} considered as *letters* and brackets (‘ and ’). The carrier $W_{\Omega_{\text{Numb}}}$ is defined by induction:

Basis of induction: The *one-letter words* **zero** and **one** belong to $W_{\Omega_{\text{Numb}}}$.

Step of induction: if the words t and s belong to $W_{\Omega_{\text{Numb}}}$, then the words $(t + s)$ and $(t \mathbf{X} s)$ belong to $W_{\Omega_{\text{Numb}}}$.

No other words belongs to $W_{\Omega_{\text{Numb}}}$.

So the basic expressions of $W_{\Omega_{\text{Numb}}}$ are the one-letter words **zero** and **one**. The complex expressions are produced from the simpler ones considered as operands and a symbol of operations and brackets: **(zero + zero)**, **(zero + one)**, **(zero X zero)**, etc. For example, applying operation **X** to operands **(zero + zero)** and **zero** we get the word **((zero + zero) X zero)** as the result. Expressions of word algebras are also called *terms*.

The **operations** of the word algebra $\mathbf{W}_{\Omega_{\text{Numb}}}$ are defined in a natural way:

zero = ‘zero’

one = ‘one’

‘zero’ + ‘zero’ = ‘(zero + zero)’

‘zero’ + ‘one’ = ‘(zero + one)’

...

‘(zero + zero) X zero’ = ‘((zero + zero) X zero)’, etc.

In the “table” above we use quotation signs as metasymbols to mark expressions as operands and results of operations.

The most important property of the word algebra is that a given result can be obtained in only one way; the terms themselves show us what operations must have been used to obtain them.

General case. For the signature Ω the word algebra \mathbf{W}_{Ω} can be defined in the same way.

The carrier W_{Ω} (we use the prefix form here in the definition):

- 1) if ω is a constant (0-ary symbol) from Ω then the one-letter word ω belongs to W_{Ω} .
- 2) if ω is an n-ary symbol from Ω and t_1, \dots, t_n are words from W_{Ω} then the word $\omega(t_1, \dots, t_n)$ belongs to W_{Ω} .

- 3) There are no other elements in W_{Ω} (than defined by (1) and (2)).

Words from W_{Ω} are also called *terms* of W_{Ω} .

The operations:

- 1) every 0-ary operation ω marks the one-letter word ω of W_Ω .
- 2) if ω is a symbol of n-ary operation from Ω , and t_1, \dots, t_n are words from W_Ω , then the word $\omega(t_1, \dots, t_n)$ is the result of the application of the operation ω to the n-tuple $\langle t_1, \dots, t_n \rangle$.

Note that in a case when a signature Ω does not contain 0-ary symbols, the word algebra described above will be empty. Below we will consider a more general notion of word algebra.

1.2. Word algebras and homomorphisms. Initial algebra.

Let us show that for any Ω_{Numb} -algebra \mathbf{A} there exists a unique homomorphism $f: \mathbf{W}_{\Omega_{\text{Numb}}} \rightarrow \mathbf{A}$. The function f can be defined by induction:

- 1) f maps the words **zero** and **one** from $W_{\Omega_{\text{Numb}}}$ to the elements of the carrier A of the algebra \mathbf{A} marked by corresponding constants; (for example to 0 and 1 in **Mod4**).
- 2) for any words t and s from $W_{\Omega_{\text{Numb}}}$ we put $f(t + s) = f(t) + f(s)$ and $f(t \times s) = f(t) \times f(s)$.

Example. The homomorphism $f: \mathbf{W}_{\Omega_{\text{Numb}}} \rightarrow \mathbf{Mod4}$ maps **zero** and **one** to 0 and 1. We have, for example, $f(\mathbf{zero} + \mathbf{zero}) = 0 + 0 = 0$ or
 $f((\mathbf{one} + \mathbf{one}) \times ((\mathbf{one} + \mathbf{one}) + \mathbf{one})) = f(\mathbf{one} + \mathbf{one}) \times f((\mathbf{one} + \mathbf{one}) + \mathbf{one}) =$
 $= (f(\mathbf{one}) + f(\mathbf{one})) \times (f(\mathbf{one} + \mathbf{one}) + f(\mathbf{one})) = (1 + 1) \times ((f(\mathbf{one}) + f(\mathbf{one})) + 1) = (2 \times 3) = 2.$

In the general case for any signature Ω containing constants and any Ω -algebra \mathbf{A} there exists a unique homomorphism $f: \mathbf{W}_\Omega \rightarrow \mathbf{A}$.

Each basic expression of the word algebra (0-ary symbol of Ω) is mapped onto the corresponding element of the carrier A of \mathbf{A} . Since the operations of the word algebra correspond to the operations of \mathbf{A} in the obvious way, the rest of the homomorphism is determined in the same obvious way.

Definition. \mathbf{I} is an *initial algebra* in signature Ω (an *initial Ω -algebra*), iff for any Ω -algebra \mathbf{A} there is a unique homomorphism $f: \mathbf{I} \rightarrow \mathbf{A}$.

Every (non-empty) word algebra \mathbf{W}_Ω is by definition is an initial algebra.

More examples.

Consider the signature $\Omega_{\text{Nt}} = \{\mathbf{zero}, \mathbf{suc}\}$, where **zero** is a 0-ary symbol and **suc** is a unary one. Consider four Ω_{Nt} -algebras: **Nt**, **Mod3**, **NtNt** and the word algebra $\mathbf{W}_{\Omega_{\text{Nt}}}$:

Nt	Nt = {0, 1, 2, 3, 4, ...}	zero = 0 suc (0) = 1, suc (1) = 2, suc (2) = 3, etc.
Mod3	Mod3 = {0, 1, 2}	zero = 0 suc (0) = 1, suc (1) = 2, suc (2) = 0
NtNt	NtNt = {0', 1', 2', ... 0'', 1'', 2'', ...}	zero = 0 suc (0') = 1', suc (1') = 2', ... suc (0'') = 1'', suc (1'') = 2'',

$\mathbf{W}_{\Omega\mathbf{Nt}}$ $\mathbf{W}_{\Omega\mathbf{Nt}} = \{\mathbf{zero}, \mathbf{suc}(\mathbf{zero}), \mathbf{suc}(\mathbf{suc}(\mathbf{zero})), \mathbf{suc}(\mathbf{suc}(\mathbf{suc}(\mathbf{zero}))), \dots\}$

Operations: $\mathbf{zero} = \text{'zero'}$

$\mathbf{suc}(\text{'zero'}) = \text{'suc}(\mathbf{zero})$

$\mathbf{suc}(\text{'suc}(\mathbf{zero})) = \text{'suc}(\mathbf{suc}(\mathbf{zero}))$, etc.

It is easy to see that the word algebra $\mathbf{W}_{\Omega\mathbf{Nt}}$ is an initial algebra.

Is \mathbf{NtNt} an initial algebra? Let us consider its homomorphisms to \mathbf{Nt} . In every homomorphism \mathbf{zero} should go to \mathbf{zero} , so 0' goes to 0, 1' to 1, etc. But where should we map 0''? It can go to 0, or to 1, or to 2, or to any other element. Giving a value for 0'' will determine the value for 1'', 2'', etc. So there are many possible homomorphisms from \mathbf{NtNt} to \mathbf{Nt} . Since there is not a unique homomorphism from \mathbf{NtNt} to \mathbf{Nt} , \mathbf{NtNt} cannot be an initial algebra.

And it is easy to show that there are no homomorphisms from $\mathbf{Mod3}$ to \mathbf{Nt} . [Show it]. So $\mathbf{Mod3}$ also is not an initial algebra.

But we can show that \mathbf{Nt} is an initial algebra. Every element of its carrier is a value of some term of the word algebra $\mathbf{W}_{\Omega\mathbf{Nt}}$. On the other hand, different terms have different values. So there exists an isomorphism $i: \mathbf{Nt} \rightarrow \mathbf{W}_{\Omega\mathbf{Nt}}$. For any $\Omega_{\mathbf{Nt}}$ -algebra \mathbf{A} the unique homomorphism $h: \mathbf{Nt} \rightarrow \mathbf{A}$ is defined as a composition $h = f \circ i$ where $f: \mathbf{W}_{\Omega\mathbf{Nt}} \rightarrow \mathbf{A}$ is the unique homomorphism of the word algebra $\mathbf{W}_{\Omega\mathbf{Nt}}$ to \mathbf{A} .

Theorem. If \mathbf{I} and \mathbf{I}' are both initial Ω -algebras then they are isomorphic.

2. Word algebra on a set. Free algebra.

2.1. Word algebra on a set.

Here we consider a slightly more general concept: the word algebra in the signature Ω on a given set X of variables. We denote such an algebra by $\mathbf{W}_{\Omega}(X)$.

Given a signature Ω and the set of variables X , let us define the set Term of *terms* over Ω and X . The definition will be recursive:

1. Every variable $x \in X$ is a term.
2. If t_1, \dots, t_n are terms and $\omega \in \Omega(n)$, then $\omega(t_1, \dots, t_n)$ is a term.

Note that by our definition 0-ary symbols from Ω (if any) are terms (by the second rule, when $n = 0$). So all the terms which we considered earlier (terms without variables) remain terms in the new definition. But now we have also terms with variables.

Let us again consider terms as words in the alphabet. This time the alphabet consists of variables from X , operators from Ω , and brackets and comma, considered as symbols. The set Term of terms (considered as words) will be the carrier of the algebra $\mathbf{W}_{\Omega}(X)$.

We define operations on the set Term of such words in a natural way:

If t_1, \dots, t_n are terms and $\omega \in \Omega(n)$, then the term $\omega(t_1, \dots, t_n)$ is the result of the application of the operation ω to the n -tuple $\langle t_1, \dots, t_n \rangle$.

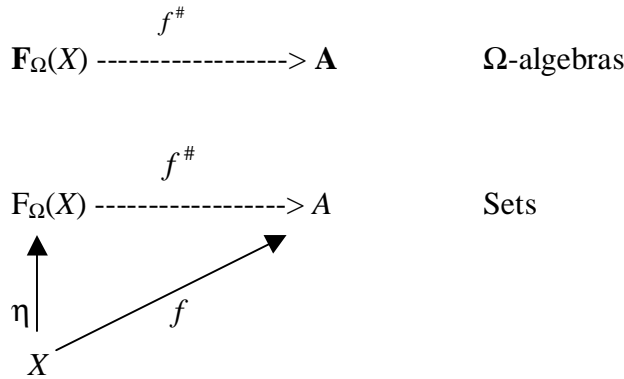
2.2. Homomorphisms from a word algebra on a set. Free algebra.

It is not difficult to show that for any Ω -algebra \mathbf{A} we have many homomorphisms from $\mathbf{W}_\Omega(X)$ to \mathbf{A} . To get such a homomorphism we should map in some way the set of variables X to the carrier A of \mathbf{A} . And we will get our homomorphism as the extension of this mapping. But we first define the abstract notion of *free* algebra with the help of this property of homomorphisms.

Definition. By a *free Ω -algebra on a set of variables X* we mean an Ω -algebra $\mathbf{F}_\Omega(X)$ with a function $\eta: X \rightarrow \mathbf{F}_\Omega(X)$, such that for any Ω -algebra \mathbf{A} any function $f: X \rightarrow A$ extends uniquely to a homomorphism $f^\#: \mathbf{F}_\Omega(X) \rightarrow \mathbf{A}$. By “ $f^\#$ extends f ” we mean that $f^\# \circ \eta = f$.

More intuitively, if $f^\#$ extends f , then $f^\#$ is identical to f wherever f is defined. And in the simplest case, η is something very close to an identity mapping (see below.)

We can illustrate the definition of free algebra $\mathbf{F}_\Omega(X)$ on a set X by a diagram:



It is easy to see that the word algebra $\mathbf{W}_\Omega(X)$ is a free algebra on X . In this case the function η is the obvious one: it maps every variable x in X to the one-letter word ‘ x ’ in Term. This is almost an identity mapping, except for the fact that x in X is just an element of a set, whereas the one-letter word ‘ x ’ in the word algebra is an element of the carrier of an algebra – they look like the same thing, but they have different ontological status.

Example. Consider the word algebra $\mathbf{W}_{\Omega_{\text{Numb}}}(X)$ in the signature Ω_{Numb} on the set of variables $X = \{x, y\}$. In this case the set Term consists of terms $x, y, \text{zero}, \text{one}, (\text{zero} + \text{zero}), (x + \text{zero}), \dots, (y \times (\text{one} + x))$, etc. (Strictly speaking we should use prefix form for terms but we will be flexible for uniformity with previous examples and traditions of arithmetic).

Let us consider the Ω_{Numb} -algebra $\mathbf{Mod4}$ and homomorphisms from $\mathbf{W}_{\Omega_{\text{Numb}}}(X)$ to $\mathbf{Mod4}$. Every such homomorphism is defined by a function $f: X \rightarrow \text{Mod4}$ ($\text{Mod4} = \{0, 1, 2, 3\}$) i.e. an evaluation of variables from X in the set Mod4 (i.e. in $\{0, 1, 2, 3\}$). And $f^\#$ is an evaluation function giving a value to every term from $\mathbf{W}_{\Omega_{\text{Numb}}}(X)$. Naturally, $f^\#(x) = f(x)$, i.e. $f^\# \circ \eta = f$.

If, for example, $f(x) = 3$ and $f(y) = 2$ then $f^\#(y \times (\text{one} + x)) = f^\#(y) \times f^\#(\text{one} + x) = f(y) \times (f^\#(\text{one}) + f^\#(x)) = 2 \times (1 + f(x)) = 2 \times (1 + 3) = 2 \times 0 = 0$.

Homework 8.2.

[This was incorrectly called Homework 8 in the first version of this handout; we already had a Homework 8 with Lecture 7. We will call this Homework 8.2.]

Note: This homework relates to Lecture 7, and does not use the notions introduced in this lecture.

1. Congruences on \mathbf{Nat} . Consider the equivalence relation $Q_{\text{Mod}4}$ “equality modulo 4” on \mathbf{N} ,
 $Q_{\text{Mod}4} = \{ \langle x, y \rangle \mid x =_{\text{Mod}4} y \}$. Do the operations from Ω_{Numb} agree with the equivalence $Q_{\text{Mod}4}$?

2. More general problem. What about “equality modulo n ” where $n \in \mathbf{N}$, $n > 1$ and the equivalence relation $Q_{\text{Mod}n} = \{ \langle x, y \rangle \mid x =_{\text{Mod}n} y \}$? Is it a congruence for every n ?