2
Preliminaries

2.1 Introduction

This second chapter introduces the basic concepts and notations related to equational theories, algebras, and term rewriting systems that are needed for the remainder of the book. Throughout the book, standard mathematical notations are used, in particular from set theory. Notation $\mathbf{N} = \{0, 1, 2, \ldots\}$ denotes the natural numbers.

2.2 Equational theories

A central notion of this book is the notion of an equational theory. An equational theory is a signature (defining a 'language') together with a set of equations over this signature (the basic laws). Every process algebra in this book is presented as a model of an equational theory, as outlined in the previous chapter.

Definition 2.2.1 (Signature) A *signature* Σ is a set of constant and function symbols with their arities.

The objects in a signature are called constant and function *symbols*. The reason for doing so is to distinguish between these purely formal objects and the 'real' constants and functions they are meant to represent. In Section 2.3, where interpretations of equational theories are discussed, this point is elaborated further. Note that a constant symbol can also be seen as a function symbol of arity zero.

Example 2.2.2 (Signature) As an example, consider the signature Σ_1 consisting of the constant symbol $\mathbf{0}$, the unary function symbol $\mathbf{s}$, and the binary function symbols $\mathbf{a}$ and $\mathbf{m}$.

Definition 2.2.3 (Terms) The set of all terms over a signature Σ and a set of variables V, notation $\mathcal{T}(\Sigma, V)$, is the smallest set that satisfies the following:

(i) each variable in V is a term in $\mathcal{T}(\Sigma, V)$;
(ii) each constant in Σ is a term in $\mathcal{T}(\Sigma, V)$;
(iii) if f is an n-ary function symbol ($n \geq 1$) and $t_1, \ldots, t_n$ are terms in $\mathcal{T}(\Sigma, V)$, then $f(t_1, \ldots, t_n)$ is a term in $\mathcal{T}(\Sigma, V)$.

In this book, it is always assumed that there are as many variables as needed. Therefore, often, the set of variables is omitted from the notation $\mathcal{T}(\Sigma, V)$, yielding the notation $\mathcal{T}(\Sigma)$ for all the terms over signature Σ. As a shorthand, terms over some signature Σ are also referred to as Σ-terms. A term that does not contain variables is called a *closed* or *ground* term. The set of all closed terms over signature Σ is denoted $\mathcal{C}(\Sigma)$. To emphasize that arbitrary terms in $\mathcal{T}(\Sigma)$ may contain variables, they are often referred to as *open* terms. Syntactical identity of terms is denoted by $\equiv$.

Definition 2.2.4 (Equational theory) An *equational theory* is a tuple (Σ, E), where Σ is a signature and E is a set of equations of the form $s = t$ where s and t are terms over this signature ($s, t \in \mathcal{T}(\Sigma)$). The equations of an equational theory are often referred to as *axioms*.

Example 2.2.5 (Equational theory) Table 2.1 gives equational theory $T_1 = (\Sigma_1, E_1)$, where Σ_1 is the signature of Example 2.2.2. The first entry of Table 2.1 lists the constant and function symbols in signature Σ_1. The second entry of the table introduces a number of variables and lists the equations in E_1. In this case, the equations of the equational theory contain variables x and y. It is assumed that variables can always be distinguished from the symbols of the signature. The equations have been given names to facilitate future reference. The attentive reader might recognize that the equations conform to the well-known axioms of *Peano arithmetic*, see e.g. (Van Heijenoort, 1967); however, strictly speaking, the symbols in the signature and the equations are still meaningless.

The objective of an equational theory is to describe which terms over the signature of this equational theory are to be considered equal. As the example equational theory shows, the equations of an equational theory often contain variables. When trying to derive equalities from a theory, it is allowed to substitute arbitrary terms for these variables.

Definition 2.2.6 (Substitution) Let Σ be a signature and V a set of variables. A *substitution* σ is a mapping from V to $\mathcal{T}(\Sigma, V)$. For any term t in $\mathcal{T}(\Sigma, V)$,

— T_1 —

constant: $\mathbf{0}$;	unary: $\mathbf{s}$;	binary: $\mathbf{a}$, $\mathbf{m}$;

x, y;

$\mathbf{a}(x, \mathbf{0})$	$=$	x	PA1
$\mathbf{a}(x, \mathbf{s}(y))$	$=$	$\mathbf{s}(\mathbf{a}(x, y))$	PA2
$\mathbf{m}(x, \mathbf{0})$	$=$	$\mathbf{0}$	PA3
$\mathbf{m}(x, \mathbf{s}(y))$	$=$	$\mathbf{a}(\mathbf{m}(x, y), x)$	PA4

Table 2.1. The equational theory $T_1 = (\Sigma_1, E_1)$.

$t[\sigma]$ denotes the term obtained by the simultaneous substitution of all variables in t according to σ. That is,

(i) for each variable x in V, $x[\sigma] = \sigma(x)$,
(ii) for each constant c in Σ, $c[\sigma] = c$, and
(iii) for any n-ary function symbol f ($n \geq 1$) and terms $t_1, \ldots, t_n$ in $\mathcal{T}(\Sigma, V)$, $f(t_1, \ldots, t_n)[\sigma]$ is the term $f(t_1[\sigma], \ldots, t_n[\sigma])$.

Example 2.2.7 (Substitution) Consider the term $t \equiv \mathbf{a}(\mathbf{m}(x, y), x)$ over the signature Σ_1 of Example 2.2.2. Let σ_1 be the substitution mapping x to $\mathbf{s}(\mathbf{s}(\mathbf{0}))$ and y to $\mathbf{0}$. Then, $t[\sigma_1]$ is the term $\mathbf{a}(\mathbf{m}(\mathbf{s}(\mathbf{s}(\mathbf{0})), \mathbf{0}), \mathbf{s}(\mathbf{s}(\mathbf{0})))$. Let σ_2 be the substitution mapping x to $\mathbf{s}(\mathbf{s}(y))$ and y to x; $t[\sigma_2]$ is the term $\mathbf{a}(\mathbf{m}(\mathbf{s}(\mathbf{s}(y)), x), \mathbf{s}(\mathbf{s}(y)))$.

There is a standard collection of proof rules for deriving equalities from an equational theory. Together, these rules define the notion of *derivability* and they are referred to as the rules of *equational logic*.

Definition 2.2.8 (Derivability) Let $T = (\Sigma, E)$ be an equational theory; let V be a set of variables and let s and t be terms in $\mathcal{T}(\Sigma, V)$. The equation $s = t$ is derivable from theory T, denoted $T \vdash s = t$, if and only if it follows from the following rules:

(Axiom rule) for any equation $s = t \in E$,
$T \vdash s = t$;
(Substitution) for any terms $s, t \in \mathcal{T}(\Sigma, V)$ and any substitution $\sigma : V \to \mathcal{T}(\Sigma, V)$,
$T \vdash s = t$ implies that $T \vdash s[\sigma] = t[\sigma]$;
(Reflexivity) for any term $t \in \mathcal{T}(\Sigma, V)$,
$T \vdash t = t$;
(Symmetry) for any terms $s, t \in \mathcal{T}(\Sigma, V)$,
$T \vdash s = t$ implies that $T \vdash t = s$;

https://doi.org/10.1017/CBO9781139195003.006 Published online by Cambridge University Press

(Transitivity) for any terms $s, t, u \in \mathcal{T}(\Sigma, V)$,

$$T \vdash s = t \text{ and } T \vdash t = u \text{ implies that } T \vdash s = u;$$

(Context rule) for any n-ary function symbol $f \in \Sigma$ $(n \geq 1)$, any terms $s, t_1, \ldots, t_n \in \mathcal{T}(\Sigma, V)$, and any natural number i with $1 \leq i \leq n$,

$$T \vdash t_i = s \text{ implies that}$$
$$T \vdash f(t_1, \ldots, t_n) = f(t_1, \ldots, t_{i-1}, s, t_{i+1}, \ldots, t_n).$$

Example 2.2.9 (Derivability) Consider equational theory $T_1 = (\Sigma_1, E_1)$ of Example 2.2.5. The following derivation shows that $T_1 \vdash \mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{s}(\mathbf{0})) = \mathbf{s}(\mathbf{s}(\mathbf{0}))$. Let σ be the substitution that maps x to $\mathbf{s}(\mathbf{0})$ and y to $\mathbf{0}$.

1. $T_1 \vdash \mathbf{a}(x, \mathbf{s}(y)) = \mathbf{s}(\mathbf{a}(x, y))$ (Axiom PA2)
2. $T_1 \vdash \mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{s}(\mathbf{0})) = \mathbf{s}(\mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{0}))$ (line 1: substitution σ)
3. $T_1 \vdash \mathbf{a}(x, \mathbf{0}) = x$ (Axiom PA1)
4. $T_1 \vdash \mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{0}) = \mathbf{s}(\mathbf{0})$ (line 3: substitution σ)
5. $T_1 \vdash \mathbf{s}(\mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{0})) = \mathbf{s}(\mathbf{s}(\mathbf{0}))$ (line 4: context rule)
6. $T_1 \vdash \mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{s}(\mathbf{0})) = \mathbf{s}(\mathbf{s}(\mathbf{0}))$ (lines 2 and 5: transitivity)

The derivation above is presented in a linear, line-based way. However, derivations are often easier to read if presented as a tree. Figure 2.1 visualizes the above tree as a so-called proof tree. In this case, the proof tree makes it explicit that the end result depends on two independent initial applications of basic axioms.

$$\dfrac{\dfrac{\dfrac{(\text{Ax. PA2})}{\mathbf{a}(x, \mathbf{s}(y)) = \mathbf{s}(\mathbf{a}(x, y))}}{\mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{s}(\mathbf{0})) = \mathbf{s}(\mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{0}))}\,(\text{sub. } \sigma) \qquad \dfrac{\dfrac{\dfrac{(\text{Ax. PA1})}{\mathbf{a}(x, \mathbf{0}) = x}}{\mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{0}) = \mathbf{s}(\mathbf{0})}\,(\text{sub. } \sigma)}{\mathbf{s}(\mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{0})) = \mathbf{s}(\mathbf{s}(\mathbf{0}))}\,(\text{cont. rule})}{\mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{s}(\mathbf{0})) = \mathbf{s}(\mathbf{s}(\mathbf{0}))}\,(\text{trans.})$$

Fig. 2.1. A proof tree.

Of course, independent of the precise representation, it is not always very practical to give derivations with the level of detail as above. In the remainder, derivations are given in a more compact form. The above derivation, for example, can be reduced as follows:

$$T_1 \vdash \mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{s}(\mathbf{0})) = \mathbf{s}(\mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{0})) = \mathbf{s}(\mathbf{s}(\mathbf{0})).$$

Note the difference between syntactical identity, as introduced in Definition 2.2.3, and derivability. Based on the reflexivity of derivability, syntactical identity implies derivability. For example, $\mathbf{s}(\mathbf{0}) \equiv \mathbf{s}(\mathbf{0})$ and $T_1 \vdash \mathbf{s}(\mathbf{0}) = \mathbf{s}(\mathbf{0})$. The converse is not true: $T_1 \vdash \mathbf{a}(\mathbf{0}, \mathbf{0}) = \mathbf{0}$ but not $\mathbf{a}(\mathbf{0}, \mathbf{0}) \equiv \mathbf{0}$.

Inductive proof techniques play an important role in the context of equational theories. They are often applicable for proving properties of (closed) terms over the signature of a theory. The example equational theory $T_1 = (\Sigma_1, E_1)$ of Table 2.1 can be used for demonstrating inductive proof techniques. The notion of so-called basic terms plays an important role in the examples that are given below. The reason why the terms are called *basic* terms becomes clear further on.

Definition 2.2.10 (Basic Σ_1-terms) Consider signature Σ_1 of Example 2.2.2. The set of *basic* Σ_1-terms is the smallest set $\mathcal{B}(\Sigma_1)$ such that (i) $\mathbf{0} \in \mathcal{B}(\Sigma_1)$ and (ii) $p \in \mathcal{B}(\Sigma_1)$ implies $\mathbf{s}(p) \in \mathcal{B}(\Sigma_1)$.

Note that this definition implies that the set of basic Σ_1-terms contains precisely all closed Σ_1-terms that can be written as $\mathbf{s}^n(\mathbf{0})$ for some $n \in \mathbf{N}$ where

$$\begin{aligned} \mathbf{s}^0(\mathbf{0}) &= \mathbf{0} \quad \text{and} \\ \mathbf{s}^{n+1}(\mathbf{0}) &= \mathbf{s}(\mathbf{s}^n(\mathbf{0})) \quad (\text{for } n \in \mathbf{N}). \end{aligned} \tag{2.2.1}$$

The first inductive proof technique that is commonly used in the context of equational theories is standard natural induction.

Example 2.2.11 (Natural induction) Consider the following property of *basic* Σ_1-terms in the context of equational theory $T_1 = (\Sigma_1, E_1)$ of Table 2.1. It uses the notation for basic terms introduced in (2.2.1).

$$\begin{aligned} &\text{For any } p, q \in \mathcal{B}(\Sigma_1) \text{ with } p = \mathbf{s}^m(\mathbf{0}) \text{ and } q = \mathbf{s}^n(\mathbf{0}), \\ &\quad T_1 \vdash \mathbf{a}(p, q) = \mathbf{s}^{m+n}(\mathbf{0}). \end{aligned} \tag{2.2.2}$$

The proof of (2.2.2) goes via *natural* induction on the *number of function symbols* in basic term q. In other words, the proof uses induction on n.

(Base case) Assume that $n = 0$, which means that $q \equiv \mathbf{0}$. From (2.2.1) and Axiom PA1, it easily follows that for all $m \in \mathbf{N}$

$$\begin{aligned} T_1 \vdash \mathbf{a}(p, q) &= \mathbf{a}(\mathbf{s}^m(\mathbf{0}), \mathbf{s}^0(\mathbf{0})) = \mathbf{a}(\mathbf{s}^m(\mathbf{0}), \mathbf{0}) = \mathbf{s}^m(\mathbf{0}) \\ &= \mathbf{s}^{m+n}(\mathbf{0}). \end{aligned}$$

(Inductive step) Assume that (2.2.2) holds for all n at most k (with $k \in \mathbf{N}$). It follows from (2.2.1) and Axiom PA2 that for all $m \in \mathbf{N}$

$$\begin{aligned} T_1 \vdash \mathbf{a}(p, q) &= \mathbf{a}(\mathbf{s}^m(\mathbf{0}), \mathbf{s}^{k+1}(\mathbf{0})) = \mathbf{s}(\mathbf{a}(\mathbf{s}^m(\mathbf{0}), \mathbf{s}^k(\mathbf{0}))) \\ &= \mathbf{s}(\mathbf{s}^{m+k}(\mathbf{0})) = \mathbf{s}^{m+k+1}(\mathbf{0}). \end{aligned}$$

By induction, it may be concluded that (2.2.2) is true for all (m and) n in $\mathbf{N}$.

It is possible to formulate a property for the $\mathbf{m}$ function symbol in signature Σ_1 that is very similar to property (2.2.2):

$$\begin{aligned} &\text{For any } p, q \in \mathcal{B}(\Sigma_1) \text{ with } p = \mathbf{s}^m(\mathbf{0}) \text{ and } q = \mathbf{s}^n(\mathbf{0}), \\ &\quad T_1 \vdash \mathbf{m}(p, q) = \mathbf{s}^{mn}(\mathbf{0}). \end{aligned} \tag{2.2.3}$$

The proof of property (2.2.3) also goes via induction on the number of function symbols of term q; it is left as Exercise 2.2.4.

Another important inductive proof technique is *structural* induction. Structural induction is a variant of natural induction that is particularly well suited for proving properties of closed terms over some signature.

Definition 2.2.12 (Structural induction) Let Σ be a signature. Let $P(t)$ be some property on terms over Σ. If,

(Base cases) for any constant symbol c in Σ,
$P(c)$
and

(Inductive steps) for any n-ary ($n \geq 1$) function symbol f in Σ and closed terms $p_1, \ldots, p_n$ in $\mathcal{C}(\Sigma)$,
the assumption that for all natural numbers i, with $1 \leq i \leq n$, $P(p_i)$ holds implies that $P(f(p_1, \ldots, p_n))$,

then $P(p)$ for any closed Σ-term p.

The following example illustrates structural induction in the context of equational theories.

Example 2.2.13 (Structural induction and elimination) Consider again the equational theory $T_1 = (\Sigma_1, E_1)$ of Example 2.2.5. An interesting property is the following so-called *elimination* property: any closed Σ_1-term can be written as a *basic* Σ_1-term as introduced in Definition 2.2.10. Since any basic term is a composition of $\mathbf{s}$ function symbols applied to the $\mathbf{0}$ constant symbol, this implies that the $\mathbf{a}$ and $\mathbf{m}$ function symbols can be eliminated from any closed term. At this point, it should be clear why the terms introduced in Definition 2.2.10 are called *basic* terms.

For any p in $\mathcal{C}(\Sigma_1)$, there is some $p_1 \in \mathcal{B}(\Sigma_1)$ such that $T_1 \vdash p = p_1$. (2.2.4)

The proof uses structural induction on the structure of closed term p.

(Base case) Assume that $p \equiv \mathbf{0}$. Since $\mathbf{0}$ is a basic Σ_1-term, the base case is trivially satisfied.

(Inductive steps)

(i) Assume $p \equiv \mathbf{s}(q)$, for some closed term $q \in \mathcal{C}(\Sigma_1)$. By induction, it may be assumed that there is some basic term $q_1 \in \mathcal{B}(\Sigma_1)$ such that $T_1 \vdash q = q_1$. Thus,
$$T_1 \vdash p = \mathbf{s}(q) = \mathbf{s}(q_1).$$
Clearly, because q_1 is a basic Σ_1-term, also $\mathbf{s}(q_1)$ is a basic term.

https://doi.org/10.1017/CBO9781139195003.006 Published online by Cambridge University Press

(ii) Assume $p \equiv \mathbf{a}(q, r)$, for some $q, r \in \mathcal{C}(\Sigma_1)$. Let $q_1, r_1 \in \mathcal{B}(\Sigma_1)$ be basic terms such that $T_1 \vdash q = q_1$ and $T_1 \vdash r = r_1$; furthermore, based on (2.2.1), assume that $m, n \in \mathbf{N}$ are natural numbers such that $q_1 = \mathbf{s}^m(\mathbf{0})$ and $r_1 = \mathbf{s}^n(\mathbf{0})$. Using (2.2.2) of Example 2.2.11, it follows that

$$T_1 \vdash p = \mathbf{a}(q, r) = \mathbf{a}(\mathbf{s}^m(\mathbf{0}), \mathbf{s}^n(\mathbf{0})) = \mathbf{s}^{m+n}(\mathbf{0}),$$

which is a basic Σ_1-term.

(iii) Assume $p \equiv \mathbf{m}(q, r)$, for some $q, r \in \mathcal{C}(\Sigma_1)$. Let $q_1, r_1 \in \mathcal{B}(\Sigma_1)$ be basic terms such that $T_1 \vdash q = q_1$ and $T_1 \vdash r = r_1$; assume that $m, n \in \mathbf{N}$ are natural numbers such that $q_1 = \mathbf{s}^m(\mathbf{0})$ and $r_1 = \mathbf{s}^n(\mathbf{0})$. Using (2.2.3), it follows that

$$T_1 \vdash p = \mathbf{m}(q, r) = \mathbf{m}(\mathbf{s}^m(\mathbf{0}), \mathbf{s}^n(\mathbf{0})) = \mathbf{s}^{mn}(\mathbf{0}).$$

Based on Definition 2.2.12, it is now valid to conclude that property (2.2.4) is true for all closed Σ_1-terms.

It is often necessary or useful to extend an equational theory with additional constant and/or function symbols and/or axioms.

Definition 2.2.14 (Extension of an equational theory) Consider two equational theories $T_1 = (\Sigma_1, E_1)$ and $T_2 = (\Sigma_2, E_2)$. Theory T_2 is an *extension* of theory T_1 if and only if Σ_2 contains Σ_1 and E_2 contains E_1.

Example 2.2.15 (Extension of an equational theory) Table 2.2 describes the extension of equational theory T_1 of Example 2.2.5 with an extra binary function symbol $\mathbf{e}$. The first entry of Table 2.2 simply says that theory T_2 extends theory T_1. The other two entries of Table 2.2 list the *new* constant and function symbols in the signature of the extended theory, one symbol in this particular example, and the new axioms.

T_2			
T_1;			
binary: $\mathbf{e}$;			
x, y;			
$\mathbf{e}(x, \mathbf{0})$	$=$	$\mathbf{s}(\mathbf{0})$	PA5
$\mathbf{e}(x, \mathbf{s}(y))$	$=$	$\mathbf{m}(\mathbf{e}(x, y), x)$	PA6

Table 2.2. The equational theory $T_2 = (\Sigma_2, E_2)$.

It is often desirable that an extension of an equational theory such as the one of Example 2.2.15 satisfies the property that it does not influence what

https://doi.org/10.1017/CBO9781139195003.006 Published online by Cambridge University Press

equalities can be derived from the original theory. Observe that the requirement on the axioms in Definition 2.2.14 (Extension) already guarantees that any equalities that are derivable in the original theory are also derivable in the extended theory. However, the addition of new axioms may result in new equalities between terms of the original syntax that could not be derived from the original axioms. An extension that does not introduce any new equalities between terms in the original syntax is said to be *conservative*.

Definition 2.2.16 (Conservative extension) Let $T_1 = (\Sigma_1, E_1)$ and $T_2 = (\Sigma_2, E_2)$ be equational theories. Theory T_2 is a *conservative extension* of theory T_1 if and only if

(i) T_2 is an extension of T_1 and,
(ii) for all Σ_1-terms s and t, $T_2 \vdash s = t$ implies $T_1 \vdash s = t$.

Proposition 2.2.17 (Conservative extension) Equational theory T_2 of Table 2.2 is a conservative extension of theory T_1 of Table 2.1.

The proof of Proposition 2.2.17 is deferred to Section 3.2, where it follows naturally from the results introduced in Chapter 3. An alternative proof technique would be to use term rewriting, as introduced in Section 2.4.

Definition 2.2.16 requires that equalities between arbitrary open terms are preserved. It is not always possible to achieve this. Sometimes, only a weaker property can be established: only equalities between closed (or ground) terms can be preserved. The following definitions adapt the notions of extension and conservative extension.

Definition 2.2.18 (Ground-extension) Consider two equational theories $T_1 = (\Sigma_1, E_1)$ and $T_2 = (\Sigma_2, E_2)$. Theory T_2 is a *ground*-extension of theory T_1 if and only if Σ_2 contains Σ_1 and for all closed Σ_1-terms p and q, $T_1 \vdash p = q$ implies $T_2 \vdash p = q$.

Definition 2.2.19 (Conservative ground-extension) Let $T_1 = (\Sigma_1, E_1)$ and $T_2 = (\Sigma_2, E_2)$ be equational theories. Theory T_2 is a *conservative ground-extension* of theory T_1 if and only if

(i) T_2 is a ground-extension of T_1 and,
(ii) for all closed Σ_1-terms p and q, $T_2 \vdash p = q$ implies $T_1 \vdash p = q$.

An interesting property of equational theory T_2 is that any closed Σ_2-term can be written as a basic Σ_1-term, as defined in Definition 2.2.10.

Proposition 2.2.20 (Elimination) Consider equational theory T_2 of Table 2.2. For any $p \in \mathcal{C}(\Sigma_2)$, there is a basic Σ_1-term $p_1 \in \mathcal{B}(\Sigma_1)$ such that

$$T_2 \vdash p = p_1.$$

Proof Exercise 2.2.5. □

Elimination properties such as (2.2.4) in Example 2.2.13 and Proposition 2.2.20 often substantially simplify structural-induction proofs. To prove properties for closed terms over the signatures of the example equational theories T_1 and T_2, it now suffices to prove these properties for basic Σ_1-terms.

Example 2.2.21 (Structural induction and elimination) Consider the equational theory $T_2 = (\Sigma_2, E_2)$ of Example 2.2.15. An interesting property of closed Σ_2-terms is the following *commutativity* property for the $\mathbf{a}$ symbol.

For any closed terms $p, q \in \mathcal{C}(\Sigma_2)$, (2.2.5)

$$T_2 \vdash \mathbf{a}(p, q) = \mathbf{a}(q, p).$$

Consider (2.2.5) formulated in terms of basic Σ_1-terms:

For any *basic* terms $p_1, q_1 \in \mathcal{B}(\Sigma_1)$, (2.2.6)

$$T_2 \vdash \mathbf{a}(p_1, q_1) = \mathbf{a}(q_1, p_1).$$

Let p and q be some closed terms in $\mathcal{C}(\Sigma_2)$. Proposition 2.2.20 (Elimination) yields that there are basic terms $p_1, q_1 \in \mathcal{B}(\Sigma_1)$ such that

$$T_2 \vdash p = p_1 \text{ and } T_2 \vdash q = q_1.$$

Assuming that it is possible to prove (2.2.6), it follows that

$$T_2 \vdash \mathbf{a}(p, q) = \mathbf{a}(p_1, q_1) = \mathbf{a}(q_1, p_1) = \mathbf{a}(q, p),$$

which proves (2.2.5).

It remains to prove (2.2.6). It is straightforward to prove (2.2.6) using property (2.2.2). However, the purpose of this example is to show a proof that goes solely via induction on the structure of basic terms and does not use property (2.2.2) which is proven via natural induction. Note that basic terms are (closed) terms over a signature that is (usually) strictly smaller than the signature of the equational theory under consideration. In the case of basic Σ_1-terms, the reduced signature consists of the constant symbol $\mathbf{0}$ and the function symbol $\mathbf{s}$, whereas the signature of Σ_2 contains the additional symbols $\mathbf{a}$, $\mathbf{m}$, and $\mathbf{e}$. It is clear that the fewer symbols a signature contains, the fewer cases need to be considered in an induction proof.

The following auxiliary properties are needed.

For any closed term $p \in \mathcal{C}(\Sigma_2)$, (2.2.7)

$$T_2 \vdash \mathbf{a}(\mathbf{0}, p) = p$$

https://doi.org/10.1017/CBO9781139195003.006 Published online by Cambridge University Press

and

$$\text{For any closed terms } p, q \in \mathcal{C}(\Sigma_2), \qquad T_2 \vdash \mathbf{a}(p, \mathbf{s}(q)) = \mathbf{a}(\mathbf{s}(p), q). \tag{2.2.8}$$

Both these properties can be proven using Proposition 2.2.20 and structural induction on *basic* terms (or (2.2.2)). Since the proofs are straightforward, they are deferred to the exercises. The proof of the commutativity property for basic terms is now as follows. Let $p_1, q_1 \in \mathcal{B}(\Sigma_1)$. The proof goes via induction on the structure of basic term q_1.

(Base case) Assume that $q_1 \equiv \mathbf{0}$. Using (2.2.7), it follows that

$$T_2 \vdash \mathbf{a}(p_1, \mathbf{0}) = p_1 = \mathbf{a}(\mathbf{0}, p_1).$$

(Inductive step) Assume that $q_1 \equiv \mathbf{s}(q_2)$ for some $q_2 \in \mathcal{B}(\Sigma_1)$. Assume that the desired commutativity property holds for term q_2, i.e., assume that $\mathbf{a}(p_1, q_2) = \mathbf{a}(q_2, p_1)$. Using (2.2.8), it follows that

$$\begin{aligned} T_2 \vdash \mathbf{a}(p_1, q_1) &= \mathbf{a}(p_1, \mathbf{s}(q_2)) = \mathbf{s}(\mathbf{a}(p_1, q_2)) = \mathbf{s}(\mathbf{a}(q_2, p_1)) \\ &= \mathbf{a}(q_2, \mathbf{s}(p_1)) = \mathbf{a}(\mathbf{s}(q_2), p_1) = \mathbf{a}(q_1, p_1). \end{aligned}$$

By induction, it may be concluded that (2.2.6) is true for all basic Σ_1-terms.

In the remainder, to improve readability, the distinction between base cases and inductive steps in structural-induction proofs is not always made explicit.

Exercises

2.2.1 Consider the equational theory $T_1 = (\Sigma_1, E_1)$ of Example 2.2.5. Give a proof tree for the fact $T_1 \vdash \mathbf{m}(\mathbf{s}(\mathbf{0}), \mathbf{s}(\mathbf{0})) = \mathbf{s}(\mathbf{0})$.

2.2.2 Consider again equational theory T_1 of Example 2.2.5. Is it true that $T_1 \vdash \mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{s}(\mathbf{0})) = \mathbf{s}(\mathbf{0})$? Can you *prove* your answer via equational logic (see Definition 2.2.8 (Derivability))? Motivate your answer.

2.2.3 Consider the following equational theory:

Fun

unary: F;

x;

$F(F(F(x)))$	$=$	x	E1
$F(F(F(F(F(x)))))$	$=$	x	E2

Show that for all (open) terms t, $Fun \vdash F(t) = t$.

2.2.4 Prove property (2.2.3) in Example 2.2.11.
(Hint: use natural induction and property (2.2.2) in Example 2.2.11.)

2.2.5 Prove Proposition 2.2.20.
(Hint: see Examples 2.2.11 and 2.2.13, and Exercise 2.2.4.)

2.2.6 Prove (2.2.7) and (2.2.8) using Proposition 2.2.20 and structural induction on basic terms.
(Hint: see Example 2.2.21.)

2.2.7 Consider equational theory T_2 of Table 2.2. Prove that, for any open terms $s, t \in \mathcal{T}(\Sigma_2)$ and closed term $p \in \mathcal{C}(\Sigma_2)$,
$$T_2 \vdash \mathbf{a}(s, \mathbf{a}(t, p)) = \mathbf{a}(\mathbf{a}(s, t), p). \qquad \text{(associativity)}$$
(Hint: use Proposition 2.2.20 and structural induction on basic terms.)

2.2.8 Consider equational theory T_2 of Table 2.2. Prove that, for any closed terms p and q in $\mathcal{C}(\Sigma_2)$,
$$T_2 \vdash \mathbf{m}(p, q) = \mathbf{m}(q, p). \qquad \text{(commutativity)}$$
(Hint: see Example 2.2.21.)

2.2.9 Consider again equational theory T_2 of Table 2.2. Prove that, for any p, q, and r in $\mathcal{C}(\Sigma_2)$,
$$T_2 \vdash \mathbf{m}(\mathbf{a}(p, q), r) = \mathbf{a}(\mathbf{m}(p, r), \mathbf{m}(q, r)). \qquad \text{(right distributivity)}$$
(Hint: use Proposition 2.2.20, property (2.2.5) of Example 2.2.21, and Exercise 2.2.7.)

2.3 Algebras

So far, equational theories were meaningless. In this section, the meaning or *semantics* of equational theories is considered. The meaning of an equational theory is given by an *algebra*.

Definition 2.3.1 (Algebra) An algebra $\mathbb{A}$ consists of a set of elements $\mathbf{A}$ together with constants in $\mathbf{A}$ and functions on $\mathbf{A}$. The set of elements $\mathbf{A}$ of an algebra $\mathbb{A}$ is called the *universe*, *domain*, or *carrier set* of $\mathbb{A}$.

Example 2.3.2 (Algebra $\mathbb{B}$) The structure $\mathbb{B} = (\mathbf{B}, \wedge, \neg, \mathit{true})$ is the algebra of the Booleans $\mathbf{B} = \{\mathit{true}, \mathit{false}\}$, where *true* is a constant, $\neg$ is the unary negation function on Booleans and $\wedge$ is the binary conjunction function on Booleans. Usually, these functions are defined by truth tables.

Example 2.3.3 (Algebra $\mathbb{N}$) Structure $\mathbb{N} = (\mathbf{N}, +, \times, \mathit{succ}, 0)$ is the algebra of the natural numbers $\mathbf{N} = \{0, 1, 2, \ldots\}$ with the unary successor function *succ*, the well-known binary functions $+$ and $\times$, and constant 0.

Note that the notation for natural numbers introduced in this example is consistent with the notation for natural numbers throughout this book, except that the $\times$ function is usually not explicitly written.

https://doi.org/10.1017/CBO9781139195003.006 Published online by Cambridge University Press

Definition 2.3.4 (Σ-algebra) Let Σ be a signature as defined in Definition 2.2.1. An algebra $\mathbb{A}$ is called a Σ-algebra when there is a mapping from the symbols of the signature Σ into the constants and functions of the algebra that respects arities. Such a mapping is called an *interpretation*.

Example 2.3.5 (Σ-algebra) Recall from Example 2.2.2 that Σ_1 is the signature containing constant $\mathbf{0}$, unary function $\mathbf{s}$, and binary functions $\mathbf{a}$ and $\mathbf{m}$. The algebra $\mathbb{N}$ of Example 2.3.3 is a Σ_1-algebra with the interpretation ι_1 defined by

$$\begin{array}{ll} \mathbf{0} & \mapsto 0, \\ \mathbf{s} & \mapsto \mathit{succ}, \\ \mathbf{a} & \mapsto +, \text{ and} \\ \mathbf{m} & \mapsto \times. \end{array}$$

Observe that also ι_2 defined by

$$\begin{array}{ll} \mathbf{0} & \mapsto 0, \\ \mathbf{s} & \mapsto \mathit{succ}, \\ \mathbf{a} & \mapsto \times, \text{ and} \\ \mathbf{m} & \mapsto + \end{array}$$

is an interpretation that satisfies the requirement that arities are respected.

At this point, the emphasis on the distinction between constant and function *symbols*, on the one hand, and real constants and functions, on the other hand, becomes clear. A signature contains merely symbols without meaning; an algebra contains real constants and functions. The symbols in a signature are given a meaning by mapping them onto constants and functions in an algebra. The above example shows that more than one mapping is often possible.

Recall that an equational theory consists of a signature plus a set of equations (see Definition 2.2.4). The idea is to give meaning to an equational theory by interpreting the terms over the signature of the theory in an algebra, as defined above. The question arises whether an arbitrary interpretation preserving arities is suitable. The answer is, hopefully not very surprisingly, negative. An extra requirement is that the equations of the theory are in some sense true in the algebra. The following definition captures the notion of truth precisely.

Definition 2.3.6 (Validity) Let Σ be a signature, V a set of variables, and $\mathbb{A}$ a Σ-algebra with domain $\mathbf{A}$. Let ι be an interpretation of Σ into $\mathbb{A}$.

A valuation $\alpha : V \to \mathbf{A}$ is a function that maps variables in V to elements of the domain of the algebra $\mathbb{A}$. For any open term t in $\mathcal{T}(\Sigma, V)$, $\iota_\alpha(t)$ is the element of $\mathbf{A}$ obtained by replacing all constant and function symbols in t by the corresponding constants and functions in $\mathbb{A}$ according to ι and by replacing all variables in t by elements of $\mathbf{A}$ according to α. That is,

https://doi.org/10.1017/CBO9781139195003.006 Published online by Cambridge University Press

(i) for each variable x in V, $\iota_\alpha(x) = \alpha(x)$,
(ii) for each constant c in Σ, $\iota_\alpha(c) = \iota(c)$, and
(iii) for any n-ary function symbol f $(n \geq 1)$ and terms $t_1, \ldots, t_n$ in $\mathcal{T}(\Sigma, V)$, $\iota_\alpha(f(t_1, \ldots, t_n))$ is the term $\iota(f)(\iota_\alpha(t_1), \ldots, \iota_\alpha(t_n))$.

Let s and t be terms in $\mathcal{T}(\Sigma, V)$. Equation $s = t$ is *valid* in the algebra $\mathbb{A}$ under interpretation ι, notation $\mathbb{A}, \iota \models s = t$, if and only if, for all valuations $\alpha : V \to \mathbf{A}$, $\iota_\alpha(s) =_\mathbf{A} \iota_\alpha(t)$, where $=_\mathbf{A}$ is the identity on domain $\mathbf{A}$.

It is often clear from the context what interpretation from some given signature into some given algebra is meant; in such cases, the interpretation in the above notation for validity is usually omitted.

Example 2.3.7 (Validity) Consider equational theory T_1 of Example 2.2.5, the algebra $\mathbb{N} = (\mathbf{N}, +, \times, succ, 0)$ of natural numbers, and the interpretations ι_1 and ι_2 given in Example 2.3.5.

The equation $\mathbf{a}(x, y) = \mathbf{a}(y, x)$ is valid in the algebra $\mathbb{N}$ under both interpretations: $\mathbb{N}, \iota_1 \models \mathbf{a}(x, y) = \mathbf{a}(y, x)$ and $\mathbb{N}, \iota_2 \models \mathbf{a}(x, y) = \mathbf{a}(y, x)$ because both $m + n =_\mathbf{N} n + m$ and $m \times n =_\mathbf{N} n \times m$ are true for all natural numbers $m, n \in \mathbf{N}$.

On the other hand, the equation $\mathbf{a}(x, \mathbf{0}) = x$ (Axiom PA1 of the theory) is valid under interpretation ι_1, because $n + 0 =_\mathbf{N} n$ for all natural numbers $n \in \mathbf{N}$, but not valid under interpretation ι_2, since $n \times 0 =_\mathbf{N} n$ is not true in $\mathbb{N}$.

An algebra is said to be a *model* of an equational theory under some interpretation if and only if all axioms of the theory are valid in the algebra under that interpretation.

Definition 2.3.8 (Model) Let $T = (\Sigma, E)$ be an equational theory, $\mathbb{A}$ a Σ-algebra, and ι an interpretation of Σ into $\mathbb{A}$. Algebra $\mathbb{A}$ is a *model* of T with respect to interpretation ι, notation $\mathbb{A}, \iota \models T$ or $\mathbb{A}, \iota \models E$ (depending on what is most convenient), if and only if, for all equations $s = t \in E$, $\mathbb{A}, \iota \models s = t$. If $\mathbb{A}$ is a model of T it is also said that T is a *sound axiomatization* of $\mathbb{A}$.

Proposition 2.3.9 (Soundness) Let $T = (\Sigma, E)$ be an equational theory with model $\mathbb{A}$ under some interpretation ι. For all Σ-terms s and t,

$T \vdash s = t$ implies $\mathbb{A}, \iota \models s = t$.

Proof The property can be proven for derivations of arbitrary length via natural induction on the number of steps in a derivation. The details follow straightforwardly from Definitions 2.2.8 (Derivability) and 2.3.6 (Validity), and are therefore omitted. □

https://doi.org/10.1017/CBO9781139195003.006 Published online by Cambridge University Press

Example 2.3.10 (Models) Consider again the equational theory T_1 of Example 2.2.5, the algebra $\mathbb{N} = (\mathbf{N}, +, \times, succ, 0)$ of natural numbers, and the interpretations ι_1 and ι_2 given in Example 2.3.5. It is not difficult to verify that $\mathbb{N}$ is a model of T_1 under interpretation ι_1. However, it is not a model of T_1 under interpretation ι_2. Example 2.3.7 shows that Axiom PA1 is not valid under ι_2.

An equational theory usually has many models.

Example 2.3.11 (Models) Consider the following variant of the algebra of the Booleans of Example 2.3.2: $\mathbb{B}_1 = (\mathbf{B}, \wedge, \oplus, \neg, \mathit{false})$ where $\mathbf{B}$, *false*, $\neg$, and $\wedge$ are as in Example 2.3.2 and $\oplus$ is the binary *exclusive or* on Booleans. The exclusive or of two Boolean values evaluates to *true* if and only if precisely one of the two values equals *true*; that is, for $b_1, b_2 \in \mathbf{B}$, $b_1 \oplus b_2 =_{\mathbf{B}} \neg(b_1 \wedge b_2) \wedge \neg(\neg b_1 \wedge \neg b_2)$. Algebra $\mathbb{B}_1$ is a model of equational theory T_1 of Example 2.2.5 under the following interpretation:

$$\begin{array}{lll} \mathbf{0} & \mapsto & \mathit{false}\,, \\ \mathbf{s} & \mapsto & \neg\,, \\ \mathbf{a} & \mapsto & \oplus\,, \text{ and} \\ \mathbf{m} & \mapsto & \wedge\,. \end{array}$$

In order to prove that $\mathbb{B}_1$ is a model of T_1, it is necessary to show that Axioms PA1 through PA4 are valid in $\mathbb{B}_1$ under the above interpretation. Possible techniques are truth tables or Boolean algebra. The proof is left as Exercise 2.3.1.

It is also possible to obtain models of a theory by extending existing models. Adding elements to the domain of a model of a theory results in another model of the theory. This occurs, for example, in the context of extensions of an equational theory, as introduced in Definition 2.2.14 (Extension). The following corollary follows immediately from Definitions 2.2.14 and 2.3.8 (Model).

Corollary 2.3.12 (Extension) Let T_1 and T_2 be two equational theories such that T_2 is an extension of T_1. Any model $\mathbb{A}$ of T_2 is also a model of T_1, i.e., $\mathbb{A} \models T_2$ implies $\mathbb{A} \models T_1$.

Among all the models of an equational theory $T = (\Sigma, E)$, there is one special model, called the *initial algebra*, that validates precisely all equations of closed terms that are derivable from E. The initial algebra of an equational theory is an example of a so-called *quotient algebra*. To define the notion of a quotient algebra, some auxiliary definitions are needed.

Definition 2.3.13 (Equivalence) An equivalence relation on some universe of elements is a binary relation that is reflexive, symmetric, and transitive.

Example 2.3.14 (Equivalence) Let $T = (\Sigma, E)$ be some equational theory. Derivability as defined in Definition 2.2.8 is an equivalence on terms over signature Σ.

Definition 2.3.15 (Equivalence classes) Let U be some universe of elements and $\sim$ an equivalence relation on U. An *equivalence class* of an element is the set of all elements equivalent to that element: that is, for any element $u \in U$, the equivalence class of u, denoted $[u]_\sim$ is the set $\{v \in U \mid u \sim v\}$. Element u is said to be a *representative* of the equivalence class.

Definition 2.3.16 (Congruence) Let $\mathbb{A}$ be an algebra with universe of elements $\mathbf{A}$. A binary relation $\sim$ on $\mathbf{A}$ is a *congruence on* $\mathbb{A}$ if and only if it satisfies the following requirements:

(i) $\sim$ is an equivalence relation on $\mathbf{A}$ and,
(ii) for every n-ary ($n \geq 1$) function f of $\mathbb{A}$ and any elements $a_1, \ldots, a_n$, $b_1, \ldots, b_n \in \mathbf{A}$, $a_1 \sim b_1, \ldots, a_n \sim b_n$ implies that $f(a_1, \ldots, a_n) \sim f(b_1, \ldots, b_n)$.

Example 2.3.17 (Congruence) Let $T = (\Sigma, E)$ be some equational theory. The set of all Σ-terms $\mathcal{T}(\Sigma)$ forms an algebra with the constant and function symbols of Σ as its constants and functions (and the syntactical-identity relation $\equiv$ as the identity). It follows from the context rule in Definition 2.2.8 that derivability is a congruence on this term algebra.

Informally, Definition 2.3.16 states that, given some congruence on some algebra, equivalence classes of elements of the universe of the algebra can be constructed via the functions of the algebra independently of the representatives of the equivalence classes. This observation forms the basis of the following definition.

Definition 2.3.18 (Quotient algebra) Let $\mathbb{A}$ be an algebra and let $\sim$ be a congruence on $\mathbb{A}$. The *quotient* algebra $\mathbb{A}$ *modulo* $\sim$, notation $\mathbb{A}_{/\sim}$, has a universe consisting of the equivalence classes of $\mathbb{A}$ under $\sim$ and it has the following constants and functions:

(i) for each constant c of $\mathbb{A}$, $[c]_\sim$ is a constant of $\mathbb{A}_{/\sim}$;
(ii) for each n-ary function f of $\mathbb{A}$, $f_\sim$ is an n-ary function of $\mathbb{A}_{/\sim}$, where, for all $a_1, \ldots, a_n \in \mathbf{A}$,

$$f_\sim([a_1]_\sim, \ldots, [a_n]_\sim) = [f(a_1, \ldots, a_n)]_\sim.$$

An important example of a quotient algebra is the initial algebra of some given equational theory.

Definition 2.3.19 (Initial algebra) Let $T = (\Sigma, E)$ be an equational theory. Consider the algebra $\mathbb{C}(\Sigma)$ with the set $\mathcal{C}(\Sigma)$ of closed Σ-terms as its domain and the constant and function symbols of Σ as its functions and constants. Derivability is a congruence on the algebra $\mathbb{C}(\Sigma)$. The initial algebra of T, denoted $\mathbb{I}(\Sigma, E)$ is the quotient algebra $\mathbb{C}(\Sigma)$ modulo derivability.

Example 2.3.20 (Quotient/initial algebra) The elements in the domain of an initial algebra of an equational theory are sets of closed terms that are derivably equal. Consider, for example, equational theory $T_1 = (\Sigma_1, E_1)$ of Example 2.2.5. Examples of elements of the domain of $\mathbb{I}(\Sigma_1, E_1)$ are

$[\mathbf{0}]_\vdash = \{\mathbf{0}, \mathbf{a}(\mathbf{0}, \mathbf{0}), \mathbf{m}(\mathbf{0}, \mathbf{0}), \mathbf{m}(\mathbf{s}(\mathbf{0}), \mathbf{0}), \ldots\}$,
$[\mathbf{s}(\mathbf{0})]_\vdash = \{\mathbf{s}(\mathbf{0}), \mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{0}), \mathbf{m}(\mathbf{s}(\mathbf{0}), \mathbf{s}(\mathbf{0})), \ldots\}$,
$[\mathbf{s}(\mathbf{s}(\mathbf{0}))]_\vdash = \{\mathbf{s}(\mathbf{s}(\mathbf{0})), \mathbf{a}(\mathbf{s}(\mathbf{0}), \mathbf{s}(\mathbf{0})), \mathbf{m}(\mathbf{s}(\mathbf{s}(\mathbf{0})), \mathbf{s}(\mathbf{0})), \ldots\}$,
et cetera.

Figure 2.2 visualizes the domain of $\mathbb{I}(\Sigma_1, E_1)$.

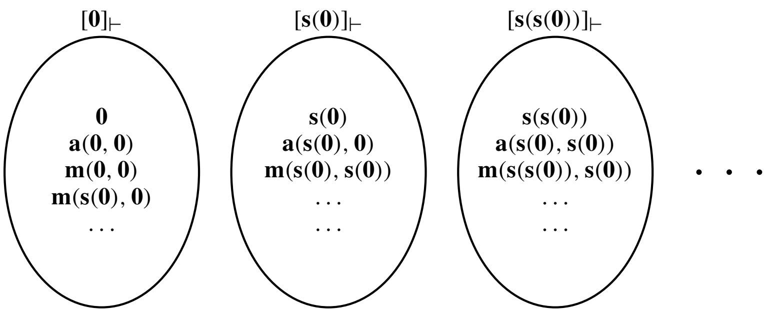

Fig. 2.2. The domain of the initial algebra of Example 2.3.20.

The constants in an initial algebra of an equational theory are the equivalence classes containing the constant symbols of the signature of the equational theory. The initial algebra $\mathbb{I}(\Sigma_1, E_1)$, for example, has one constant, namely $[\mathbf{0}]_\vdash$.

The functions in an initial algebra are obtained by lifting the function symbols in the signature of the equational theory to equivalence classes of derivably equal closed terms. Initial algebra $\mathbb{I}(\Sigma_1, E_1)$ has three functions, one unary function $\mathbf{s}_\vdash$ and two binary functions $\mathbf{a}_\vdash$ and $\mathbf{m}_\vdash$, that are defined as follows: for any closed Σ_1-terms p and q, $\mathbf{s}_\vdash([p]_\vdash) = [\mathbf{s}(p)]_\vdash$, $\mathbf{a}_\vdash([p]_\vdash, [q]_\vdash) = [\mathbf{a}(p, q)]_\vdash$, and $\mathbf{m}_\vdash([p]_\vdash, [q]_\vdash) = [\mathbf{m}(p, q)]_\vdash$.

https://doi.org/10.1017/CBO9781139195003.006 Published online by Cambridge University Press

Proposition 2.3.21 (Soundness) Let $T = (\Sigma, E)$ be an equational theory. The initial algebra $\mathbb{I}(\Sigma, E)$ is a model of T under the interpretation that maps any constant symbol c of Σ onto the equivalence class $[c]_\vdash$ and any function symbol f of Σ onto the corresponding function $f_\vdash$ as defined in Definition 2.3.18 (Quotient algebra).

Proof The property follows in a straightforward way from Definitions 2.2.8 (Derivability), 2.3.8 (Model), and 2.3.19 (Initial algebra). The details are illustrated by means of a concrete example.

Consider the equational theory $T_1 = (\Sigma_1, E_1)$. According to Definition 2.3.8 (Model), it must be shown that all axioms in E_1 are valid in the initial algebra $\mathbb{I}(\Sigma_1, E_1)$ under the interpretation ι defined above. Consider Axiom PA1: $\mathbf{a}(x, \mathbf{0}) = x$. To prove that PA1 is valid (see Definition 2.3.6 (Validity)), consider the valuation α that maps x to equivalence class $[p]_\vdash$ for some arbitrary closed Σ_1-term p. It must be shown that $\iota_\alpha(\mathbf{a}(x, \mathbf{0})) = \iota_\alpha(x)$.

The various definitions given so far imply that $\iota_\alpha(\mathbf{a}(x, \mathbf{0})) = \mathbf{a}_\vdash([p]_\vdash, [\mathbf{0}]_\vdash) = [\mathbf{a}(p, \mathbf{0})]_\vdash$ and $\iota_\alpha(x) = [p]_\vdash$. It follows from the axiom rule and the substitution rule in Definition 2.2.8 (Derivability) that $T_1 \vdash \mathbf{a}(p, \mathbf{0}) = p$. Thus, Definition 2.3.19 (Initial algebra) yields that $[\mathbf{a}(p, \mathbf{0})]_\vdash = [p]_\vdash$, proving the desired property. □

As already mentioned, the initial algebra of an equational theory is a particularly interesting model of the theory because it precisely validates all the equations of closed terms that are derivable from the axioms of the theory. This property is called ground-completeness. Since an equational theory has a standard interpretation into its initial algebra (see Proposition 2.3.21), for convenience, this interpretation is often not explicitly mentioned and it is omitted in the notations for validity and soundness.

Proposition 2.3.22 (Ground-completeness) Let $T = (\Sigma, E)$ be an equational theory. For all *closed* Σ-terms p and q,

$\mathbb{I}(\Sigma, E) \models p = q$ implies $T \vdash p = q$.

Proof The property follows from Definitions 2.3.6 (Validity) and 2.3.19 (Initial algebra). Assume that $\mathbb{I}(\Sigma, E) \models p = q$, for closed Σ-terms p and q. It follows that $[p]_\vdash = [q]_\vdash$, which implies that $T \vdash p = q$. □

Ground-completeness of a model of some theory is an interesting property because it implies that the model does not validate any equations *of closed terms* that are not also derivable from the theory. The initial algebra of an equational theory is ground-complete for that theory by definition. However,

https://doi.org/10.1017/CBO9781139195003.006 Published online by Cambridge University Press

ground-completeness is not necessarily restricted to the initial algebra of an equational theory; other models of the theory may also satisfy this property.

Definition 2.3.23 (Ground-completeness) Let $T = (\Sigma, E)$ be an equational theory with model $\mathbb{A}$ under some interpretation ι. Theory T is said to be a *ground-complete axiomatization* of model $\mathbb{A}$ if and only if, for all *closed* Σ-terms p and q,

$\mathbb{A}, \iota \models p = q$ implies $T \vdash p = q$.

Alternatively, it is said that model $\mathbb{A}$ is ground-complete for theory T.

The definition of ground-completeness is restricted to equations of *closed* terms. Of course, the property may also hold for equations of arbitrary open terms, in which case it is simply referred to as completeness.

Definition 2.3.24 (Completeness) Let $T = (\Sigma, E)$ be an equational theory with model $\mathbb{A}$ under some interpretation ι. Theory T is said to be a *complete axiomatization* of model $\mathbb{A}$ if and only if, for all *open* Σ-terms s and t,

$\mathbb{A}, \iota \models s = t$ implies $T \vdash s = t$.

It is also said that model $\mathbb{A}$ is complete for theory T.

Unfortunately, general completeness often turns out to be much more difficult to achieve than ground-completeness. Therefore, this book focuses on ground-completeness.

Example 2.3.25 (Completeness) Consider equational theory $T_1 = (\Sigma_1, E_1)$ of Example 2.2.5 and its initial algebra $\mathbb{I}(\Sigma_1, E_1)$. It has already been shown that the initial algebra is ground-complete. However, it is not complete for open terms. Consider, for example, the equation $\mathbf{a}(x, y) = \mathbf{a}(y, x)$ for variables x and y. This equation is valid in the initial algebra, $\mathbb{I}(\Sigma_1, E_1) \models \mathbf{a}(x, y) = \mathbf{a}(y, x)$, but it is not derivable; that is $T_1 \vdash \mathbf{a}(x, y) = \mathbf{a}(y, x)$ is not true. The proof of the former is left as Exercise 2.3.4. The latter can be shown by giving a model that does not validate $\mathbf{a}(x, y) = \mathbf{a}(y, x)$; if such a model exists, it follows from Proposition 2.3.9 (Soundness) that the equation cannot be derivable. Exercise 2.3.5 asks for a model of T_1 that does not validate $\mathbf{a}(x, y) = \mathbf{a}(y, x)$.

The notions of ground-completeness and completeness refer to a specific model of the theory under consideration. As a final remark concerning notions of completeness, it is interesting to observe that it is also possible to define a model-independent notion of completeness for equational theories. A theory is said to be ω-complete if and only if it is a complete axiomatization of its

https://doi.org/10.1017/CBO9781139195003.006 Published online by Cambridge University Press

initial algebra. Although this definition refers to a model, namely the initial algebra, it can be considered model-independent because the initial algebra of an equational theory is constructed in a standard way from the theory. An equivalent formulation of ω-completeness is the following: an equational theory is ω-complete if and only if an equation of arbitrary open terms is derivable when all closed-term equations obtainable from it through substitutions are derivable.

The property of ω-completeness implies that all relevant equations are fully captured by derivability. Our example theory T_1 is not ω-complete. This follows immediately from Example 2.3.25 that shows that it is not complete with respect to its initial algebra. Despite the elegance implied by the property of ω-completeness, it is not considered in the remainder of this book, and therefore the definition is not stated formally. It is often not straightforward to obtain ω-completeness.

So far, three models have been given for the example theory $T_1 = (\Sigma_1, E_1)$ of Example 2.2.5, namely the algebra of the naturals of Example 2.3.10, the algebra of the Booleans of Example 2.3.11, and the initial algebra of Example 2.3.20. This raises the question whether these models are really different.

Definition 2.3.26 (Isomorphism of algebras) Let $\mathbb{A}_1$ and $\mathbb{A}_2$ be two algebras with domains $\mathbf{A}_1$ and $\mathbf{A}_2$, respectively. Algebras $\mathbb{A}_1$ and $\mathbb{A}_2$ are *isomorphic* if and only if there exists a bijective function $\phi : \mathbf{A}_1 \to \mathbf{A}_2$ and another bijective function ψ that maps the constants and functions of $\mathbb{A}_1$ onto those of $\mathbb{A}_2$ such that

(i) for any constant c of $\mathbb{A}_1$, $\phi(c) = \psi(c)$, and
(ii) for any n-ary ($n \geq 1$) function f of $\mathbb{A}_1$ and any elements $a_1, \ldots, a_n \in \mathbf{A}_1$, $\phi(f(a_1, \ldots, a_n)) = \psi(f)(\phi(a_1), \ldots, \phi(a_n))$.

Example 2.3.27 (Isomorphism) Consider again theory $T_1 = (\Sigma_1, E_1)$ of Example 2.2.5 and its models, namely the algebra $\mathbb{N}$ of Example 2.3.10, the algebra $\mathbb{B}_1$ of Example 2.3.11, and the initial algebra $\mathbb{I}(\Sigma_1, E_1)$ of Example 2.3.20. The algebras $\mathbb{N}$ and $\mathbb{I}(\Sigma_1, E_1)$ are isomorphic (see Exercise 2.3.6). Clearly, the algebra $\mathbb{B}_1$ is not isomorphic to the other two, because its domain has only two elements whereas the domains of the other two algebras have infinitely many elements.

Usually, algebras, and in particular models of equational theories, that are isomorphic are not distinguished. Thus, the algebra of the naturals $\mathbb{N}$ of Example 2.3.10 may be referred to as the initial algebra of the equational theory $T_1 = (\Sigma_1, E_1)$ of Example 2.2.5.

Exercises

2.3.1 Consider Example 2.3.11 (Models). Show that algebra $\mathbb{B}_1$ is a model of theory T_1.

2.3.2 Verify that $\mathbb{B}_1 \models \mathbf{s}(\mathbf{m}(x, y)) = \mathbf{a}(\mathbf{a}(\mathbf{s}(x), \mathbf{s}(y)), \mathbf{m}(\mathbf{s}(x), \mathbf{s}(y)))$ for algebra $\mathbb{B}_1$ of Example 2.3.11. Does this formula also hold in algebra $\mathbb{N}$ of Example 2.3.10?

2.3.3 Consider the algebra of natural numbers $(\mathbf{N}, +, \times, exp, succ, 0)$ that extends the algebra of Example 2.3.3 with the exponentiation function *exp*. Show that this algebra is a model of theory T_2 of Example 2.2.15.

2.3.4 Consider equational theory $T_1 = (\Sigma_1, E_1)$ of Example 2.2.5 and its initial algebra $\mathbb{I}(\Sigma_1, E_1)$ of Example 2.3.20. Show that $\mathbb{I}(\Sigma_1, E_1) \models \mathbf{a}(x, y) = \mathbf{a}(y, x)$, for variables x and y.
(Hint: use property (2.2.5) and Proposition 2.2.17 (Conservative extension).)

2.3.5 Consider again equational theory $T_1 = (\Sigma_1, E_1)$ of Example 2.2.5. Give a model that does not validate the equation $\mathbf{a}(x, y) = \mathbf{a}(y, x)$, for variables x and y.
(Hint: consider an algebra where the domain consists of two elements and map the **a** function symbol onto a projection function that gives for each pair of elements the first element of the pair.)

2.3.6 Consider the algebras $\mathbb{N}$ of Example 2.3.10 and $\mathbb{I}(\Sigma_1, E_1)$ of Example 2.3.20 (the initial algebra of theory $T_1 = (\Sigma_1, E_1)$ of Example 2.2.5). Show that the two algebras are isomorphic.

2.3.7 Show that the intersection of any number of congruences is again a congruence.

2.3.8 Let $T = (\Sigma, E)$ be an equational theory. Consider the algebra of closed terms $\mathbb{C}(\Sigma)$ as introduced in Definition 2.3.19 (Initial algebra). Let $\sim$ be the intersection of all congruence relations R on $\mathbb{C}(\Sigma)$ such that $\mathbb{C}(\Sigma)_{/R} \models E$. Show that $\sim$ coincides with derivability (which implies that $\mathbb{C}(\Sigma)_{/\sim}$ is isomorphic to the initial algebra $\mathbb{I}(\Sigma, E)$).

2.4 Term rewriting systems

Although equality in an equational theory is a symmetric relation, often the equations have an implied direction. This is already the case in primary school, where $2 + 2$ is to be replaced by 4, and not the other way around. Direction in an equational theory is formalized by the notion of a term rewriting system. Term rewriting systems can also be useful in proofs, as a proof technique.