Course Notes 4
March 12
revised March 14, 2003, 826 minutes

Term Models & Equational Completeness

We can generalize the theory of Arithmetic Expressions developed in Notes 2 to other algebraic structures.

1 First-order Terms

A *signature*, Σ, specifies the names of operations and the number of arguments (*arity*) of each operation. For example, the signature of arithmetic expressions is the set of names $\{\texttt{0}, \texttt{1}, \texttt{+}, \texttt{*}, \texttt{-}\}$ with `+` and `*` each of arity two, and `-` of arity one. The constants `0` and `1` by convention are considered to be operations of arity zero.

As a running example, we will consider a signature, Σ_0, with three names: `F` of arity two, `G` of arity one, and a constant, `c`.

The *First-order Terms over* Σ are defined in essentially the same way as arithmetic expressions. We'll omit the adjective "first-order" in the rest of these notes.

Definition 1.1. The set, $\mathcal{T}_\Sigma$, of *Terms* over Σ are defined inductively as follows:

- Any variable, x, is in $\mathcal{T}_\Sigma$.[1]
- Any constant, $c \in \Sigma$, is in $\mathcal{T}_\Sigma$.
- If $f \in \Sigma$ has arity $n > 0$, and $M_1, \ldots, M_n \in \mathcal{T}_\Sigma$, then

$$f\texttt{(}M_1\texttt{,}\ \ldots\texttt{,}M_n\texttt{)} \in \mathcal{T}_\Sigma.$$

For example,

```
c, x, F(c,x), G(G(F(y,G(c))))
```

are examples of terms over Σ_0.

[1]We needn't specify exactly what variables are. All that matters is that variables are distinct from other kinds of terms and from operation names in the signature.

2 Substitution

A *substitution* over signature, Σ, is a mapping, σ, from the set of variables to $\mathcal{T}_\Sigma$. The notation

$$[x_1, \ldots, x_n := M_1, \ldots, M_n]$$

describes the substitution that maps variables $x_1, \ldots, x_n$ respectively to $M_1, \ldots, M_n$, and maps all other variables to themselves.

Definition 2.1. Every substitution, σ, defines a mapping, $[\sigma]$, from $\mathcal{T}_\Sigma$ to $\mathcal{T}_\Sigma$ defined inductively as follows:

$$\begin{aligned} x[\sigma] &::= \sigma(x) && \text{for each variable, } x. \\ c[\sigma] &::= c && \text{for each constant, } c. \\ f\texttt{(}M_1\texttt{,}\ \ldots\texttt{,}\, M_n\texttt{)}[\sigma] &::= f\texttt{(}M_1[\sigma]\texttt{,}\ \ldots\texttt{,}\, M_n[\sigma]\texttt{)} && \text{for each } f \in \Sigma \text{ of arity } n > 0. \end{aligned}$$

For example

$$\texttt{F(G(x),y)}[\texttt{x},\texttt{y} := \texttt{F(c,y)},\texttt{G(x)}] \text{ is the term } \texttt{F(G(F(c,y)),G(x))}.$$

3 Models

A model assigns meaning to terms by specifying the space of values that terms can have and the meaning of the operations named in a signature. Models are also called "first-order structures" or "algebras."

Definition 3.1. A *model*, $\mathcal{M}$, for signature, Σ, consists a nonempty set, $\mathcal{A}_\mathcal{M}$, called the *carrier* of $\mathcal{M}$, and a mapping $[\![\cdot]\!]_0$ that assigns an n-ary operation on the carrier to each symbol of arity n in Σ. That is, for each $f \in \Sigma$ of arity $n > 0$,

$$[\![f]\!]_0 : {\mathcal{A}_\mathcal{M}}^n \to \mathcal{A}_\mathcal{M},$$

and for each $c \in \Sigma$ of arity 0,

$$[\![c]\!]_0 \in \mathcal{A}_\mathcal{M}.$$

For example, a model for Σ_0 might have carrier equal to the set of binary strings, with `F` meaning the concatenation operation, `G` meaning reversal, and `c` meaning the symbol `1`.

Definition 3.2. An $\mathcal{M}$*-valuation*, V, is a mapping from variables into the carrier, $\mathcal{A}_\mathcal{M}$.

Once we have a model and valuation, we can define a value from the carrier for any term, M. The meaning, $[\![M]\!]_\mathcal{M}$, of the term itself is defined to be the function from valuations to the term's value under a valuation. We'll usually omit the subscript when it's clear which model, $\mathcal{M}$, is being referenced.

Definition 3.3. The meaning, $[\![M]\!]_{\mathcal{M}}$, of a term, M, in a model, $\mathcal{M}$, is defined by structural induction on the definition of M:

$$
\begin{aligned}
[\![x]\!]V &::= V(x) && \text{for each variable, } x.\\
[\![c]\!]V &::= [\![c]\!]_0 && \text{for each constant, } c \in \Sigma.\\
[\![f(M_1, \ldots, M_n)]\!]V &::= [\![f]\!]_0([\![M_1]\!]V, \ldots, [\![M_n]\!]V) && \text{for each } f \in \Sigma \text{ of arity } n > 0.
\end{aligned}
$$

Definition 3.4. For any function, F, and elements a, b, we define the *patch of F at a with b*, in symbols, $F[a \leftarrow b]$, to be the function, G, such that

$$G(x) = \begin{cases} b & \text{if } x = a. \\ F(x) & \text{otherwise.} \end{cases}$$

The fundamental relationship between substitution and meaning is given by

Lemma 3.5 (Substitution).

$$[\![M[x := N]]\!]V = [\![M]\!](V[x \leftarrow [\![N]\!]V]),$$

Lemma 3.5. follows by structural induction on M as in Notes 3.

Definition 3.6. An *equation* is an expression of the form $(M = N)$ where M, N are terms. The equation is *valid* in $\mathcal{M}$, written

$$\mathcal{M} \models (M = N),$$

iff $[\![M]\!] = [\![N]\!]$. If $\mathcal{E}$ is a set of equations, then $\mathcal{E}$ *is valid in* $\mathcal{M}$, written

$$\mathcal{M} \models \mathcal{E},$$

iff $\mathcal{M} \models (M = N)$ for each equation $(M = N) \in \mathcal{E}$.

Finally, $\mathcal{E}$ *logically implies* another set, $\mathcal{E}'$, of equations, written

$$\mathcal{E} \models \mathcal{E}',$$

when $\mathcal{E}'$ is valid for any model in which $\mathcal{E}$ is valid. That is, for every model, $\mathcal{M}$

$$\mathcal{M} \models \mathcal{E} \quad \text{implies} \quad \mathcal{M} \models \mathcal{E}'.$$

4 Proving Equations

There are some standard rules for proving equations over a given signature from any set, $\mathcal{E}$, of equations. The equations in $\mathcal{E}$ are called the *axioms*. We write $\mathcal{E} \vdash E$ to indicate that equation E is provable from the axioms. The proof rules are given in Table 1.

Note that a more general (congruence) rule follows from the rules above. Namely, let σ_1 and σ_2 be substitutions and define

$$\mathcal{E} \vdash (\sigma_1 = \sigma_2)$$

to mean that $\mathcal{E} \vdash (\sigma_1(x) = \sigma_2(x))$ for all variables, x.

Table 1: Standard Equational Inference Rules.

	$\Longrightarrow$	E for $E \in \mathcal{E}$.	(axiom)
	$\Longrightarrow$	$(M = M)$.	(reflexivity)
$(M = N)$	$\Longrightarrow$	$(N = M)$.	(symmetry)
$(L = M), (M = N)$	$\Longrightarrow$	$(L = N)$.	(transitivity)
$(M_1 = N_1), \ldots, (M_n = N_n)$	$\Longrightarrow$	$(f(M_1, \ldots, M_n) = f(N_1, \ldots, N_n))$ for each $f \in \Sigma$ of arity $n > 0$.	(congruence)
$(M = N)$	$\Longrightarrow$	$(M[x := L] = N[x := L])$.	(substitution)

Lemma 4.1. *If* $\mathcal{E} \vdash (\sigma_1 = \sigma_2)$*, then*

$$\mathcal{E} \vdash (M[\sigma_1] = M[\sigma_2]). \qquad \text{(general congruence)}$$

There is also a more general (substitution) rule:

Lemma 4.2. *If* $\mathcal{E} \vdash (M = N)$*, then for any substitution,* σ*,*

$$\mathcal{E} \vdash (M[\sigma] = N[\sigma]). \qquad \text{(general substitution)}$$

Problem 1. Prove that the (general congruence) rule implies (congruence).

Problem 2. **(a)** Prove the (general congruence) rule of Lemma 4.1.

(b) Prove the (general substitution) rule of Lemma 4.2. *Hint:* Prove that any substitution into a term M can be obtained by a series of one-variable substitutions, namely,

$$M[\sigma] = M[x_1 := N_1][x_2 := N_2] \ldots [x_n := N_n]$$

for some variables $x_1, x_2, \ldots, x_n$ and terms $N_1, N_2, \ldots, N_n$. There is slightly more to the proof than might be expected.

Theorem 4.3 (Soundness). *If* $\mathcal{E} \vdash (M = N)$*, then* $\mathcal{E} \models (M = N)$.

Proof. The Theorem follows by induction on the structure of the formal proof that $(M = N)$. The only nontrivial case is when $(M = N)$ is a consequence of the (substitution) rule. We show that this case follows from the Substitution Lemma 3.5.

Namely, suppose M is $(M'[x := L])$ and N is $(N'[x := L])$ where $\mathcal{E} \vdash (M' = N')$. Then by induction,

$$\mathcal{E} \models (M' = N'). \qquad (1)$$

So if $\mathcal{M}$ is any model such that $\mathcal{M} \models \mathcal{E}$, we have by definition from (1) that

$$[\![M']\!] = [\![N']\!]. \tag{2}$$

Now,

$$\begin{aligned}
[\![M]\!]V =& [\![M'[x := L]]\!]V && \text{(by def of } M'\text{)}\\
=& [\![M']\!](V[x \leftarrow [\![L]\!]V]) && \text{(by Subst. Lemma 3.5)}\\
=& [\![N']\!](V[x \leftarrow [\![L]\!]V]) && \text{(by (2))}\\
=& [\![N'[x := L]]\!]V && \text{(by Subst. Lemma 3.5)}\\
=& [\![N]\!]V && \text{(by def of } N'\text{)},
\end{aligned}$$

which shows that $[\![M]\!] = [\![N]\!]$, and hence $\mathcal{E} \models (M = N)$, as required.

□

5 Completeness

We are now ready to prove

Theorem 5.1 (Completeness). *If $\mathcal{E} \models (M = N)$, then $\mathcal{E} \vdash (M = N)$.*

We prove Theorem 5.1 by constructing a model, $\mathcal{M}_{\mathcal{E}}$, in which provable equality and semantical equality coincide. Namely, we will show that

Lemma 5.2.

$$\mathcal{E} \vdash (M = N) \quad \textit{iff} \quad \mathcal{M}_{\mathcal{E}} \models (M = N).$$

Completeness follows directly from Lemma 5.2. In particular, since $\mathcal{E} \vdash E$ by the (axiom) rule for any equation, $E \in \mathcal{E}$, Lemma 5.2 immediately implies that

$$\mathcal{M}_{\mathcal{E}} \models \mathcal{E}.$$

Moreover, if $\mathcal{E} \not\vdash (M = N)$, then $\mathcal{M}_{\mathcal{E}} \not\models (M = N)$, and so $\mathcal{E} \not\models (M = N)$.

It remains to define the model, $\mathcal{M}_{\mathcal{E}}$, and to prove Lemma 5.2. The model $\mathcal{M}_{\mathcal{E}}$ will be a term model depending only on the axioms $\mathcal{E}$, not on the particular terms M or N.

The proof rules of (reflexivity), (symmetry) and (transitivity) imply that for any fixed $\mathcal{E}$, provable equality between terms M and N is an equivalence relation. We let $[M]_{\mathcal{E}}$ be the equivalence class of M under provable equality, that is,

$$[M]_{\mathcal{E}} ::= \{N \mid \mathcal{E} \vdash (M = N)\}.$$

So we have by definition

$$\mathcal{E} \vdash (M = N) \qquad \text{iff} \qquad [M]_{\mathcal{E}} = [N]_{\mathcal{E}}. \tag{3}$$

The carrier of $\mathcal{M}_{\mathcal{E}}$ will be defined to be the set of $[M]_{\mathcal{E}}$ for $M \in \mathcal{T}_{\Sigma}$. The meaning of constants, $c \in \Sigma$, will be

$$[\![c]\!]_0 ::= [c]_{\mathcal{E}}.$$

The meaning of operations $f \in \Sigma$ of arity $n > 0$ will be

$$[\![f]\!]_0([M_1]_{\mathcal{E}}, \ldots [M_n]_{\mathcal{E}}) ::= [f\texttt{(}M_1\texttt{,} \ \ldots \texttt{,} M_n\texttt{)}]_{\mathcal{E}}.$$

Notice that $[\![f]\!]_0$ applied to the equivalence classes $[M_1]_{\mathcal{E}}, \ldots [M_n]_{\mathcal{E}}$ is defined in terms of the designated terms $M_1, \ldots, M_n$ in these classes. To be sure that $[\![f]\!]_0$ is well-defined, we must check that the value of $[\![f]\!]_0$ would not change if we chose other designated terms in these classes. That is, we must verify that

$$\text{if } [M_1]_{\mathcal{E}} = [N_1]_{\mathcal{E}}, \ldots, [M_n]_{\mathcal{E}} = [N_n]_{\mathcal{E}}, \text{ then } [f\texttt{(}M_1, \ldots, M_n\texttt{)}]_{\mathcal{E}} = [f\texttt{(}N_1, \ldots, N_n\texttt{)}]_{\mathcal{E}}.$$

But this is an immediate consequence of the (congruence) rule.

For any substitution, σ, let V_σ be the $\mathcal{M}$-valuation given by

$$V_\sigma(x) ::= [\sigma(x)]_{\mathcal{E}}$$

for all variables, x. The following key property of the term model follows by structural induction on terms, M.

Lemma 5.3.

$$[\![M]\!]V_\sigma = [M[\sigma]]_{\mathcal{E}}.$$

Problem 3. Prove Lemma 5.3.

Now let ι be the identity substitution $\iota(x){::=}x$ for all variables, x. For any term, M, the substitution instance $M[\iota]$ is simply identical to M, so Lemma 5.3 immediately implies

$$[\![M]\!]V_\iota = [M]_{\mathcal{E}}.$$

In particular, if $[\![M]\!] = [\![N]\!]$, then $[M]_{\mathcal{E}} = [N]_{\mathcal{E}}$, so from equation (3), we conclude Lemma 5.2 in the right-to-left direction:

Corollary 5.4. *If $[\![M]\!]_{\mathcal{M}_{\mathcal{E}}} = [\![N]\!]_{\mathcal{M}_{\mathcal{E}}}$, then $\mathcal{E} \vdash \texttt{(}M \ \texttt{=} \ N\texttt{)}$.*

Finally, for the left-to-right direction of Lemma 5.2, we prove

Corollary 5.5. *If $\mathcal{E} \vdash \texttt{(}M \ \texttt{=} \ N\texttt{)}$, then $[\![M]\!]_{\mathcal{M}_{\mathcal{E}}} = [\![N]\!]_{\mathcal{M}_{\mathcal{E}}}$.*

Proof. If $\mathcal{E} \vdash \texttt{(}M \ \texttt{=} \ N\texttt{)}$, then by (general substitution) $\mathcal{E} \vdash \texttt{(}M[\sigma] \ \texttt{=} \ N[\sigma]\texttt{)}$ for any substitution, σ. So

$$[M[\sigma]]_{\mathcal{E}} = [N[\sigma]]_{\mathcal{E}} \tag{4}$$

by (3). Now let V be any $\mathcal{M}$-valuation, and let σ be any substitution such that $\sigma(x) \in V(x)$ for all variables, x. This ensures that

$$V = V_\sigma, \tag{5}$$

and we have

$$\begin{aligned}
[\![M]\!]V &= [M[\sigma]]_{\mathcal{E}} && \text{(by (5) \& Lemma 5.3)}\\
&= [N[\sigma]]_{\mathcal{E}} && \text{(by (4))}\\
&= [\![N]\!]V && \text{(by (5) \& Lemma 5.3).}
\end{aligned}$$

Since V was an arbitrary valuation, we conclude that $[\![M]\!] = [\![N]\!]$, as required. □