Formal Methods / Nachum Dershowitz
Lecture 6, 11-04-2000
Notes by: Sivan Sabato

Algebraic Semantics

Introduction

We can define the requirements from a program that computes a function, with a set of axioms of equality. For example, we can specify the requirements from a program that computes addition of natural numbers using the following set of axioms, which will be denoted E_a:

$$\begin{array}{lrcl} \forall x & x+0 & = & x \\ \forall x,y & x+s(y) & = & s(x+y) \end{array}$$

These axioms can also be used as directional rewrite rules to actually compute the result of addition:

$$\begin{array}{lrcl} \forall x & x+0 & \to & x \\ \forall x,y & x+s(y) & \to & s(x+y) \end{array}$$

Although E_a correctly computes addition, not all equalities concerning addition that hold over the natural numbers can be derived from E_a. For example: using E_a we can prove by induction that $s^m0+s^n0=s^n0+s^m0$, but the general law of commutativity: $x+y=y+x$ cannot be derived from these axioms: $E_a \nvdash x+y=y+x$. This is because there are models of E_a where this law does not hold: $E_a \nvDash x+y=y+x$.
An example of such a model is one that contains two types of objects: red numbers and blue numbers. The red numbers are the successors of 0_{red}, and the blue numbers are the successors of 0_{blue}. Addition is defined such that $x_{red}+y_{blue}=(x+y)_{red}$ and $x_{blue}+y_{red}=(x+y)_{blue}$. This non-standard model of numbers satisfies both axioms (mapping 0 to either 0_{red} or 0_{blue} and S to the successor function), but not the law of commutativity.
Another example of an equality that holds for natural numbers but not for all the models of E_a is $0+x=x$.

Suppose we wanted to verify that a certain program for computing addition does, in fact comply with our requirements. Then, if we used only the axioms in E_a, an implementation that uses the equality $0 + x = x$ would be regarded false, because it does not comply with al the models of E_a. This is contrary to the fact that when we defined E_a we had in mind a specific model in which this equality is valid, and therefore, should be allowed.

Formal Definitions

We discuss inference systems over the equality relation, with the following inference rules:

$$\begin{aligned} x = y &\rightarrow y = x \\ x = y \wedge y = z &\rightarrow x = z \\ x = y &\rightarrow fx = fy \end{aligned}$$

Let $\mathcal{T}$ be all terms constructed from function symbols $\mathcal{F}$ and variables $\mathcal{X}$, and let E be a set of equalities over $\mathcal{T}$. We have the following theorem:

Theorem 1 (Completeness) *For any set of equations E and terms s and t in $\mathcal{T}$, $\mathcal{M}od(E) \models s = t$ iff $E \vdash s = t$.*

In other words, all equalities that are true for all the models of E can be proven and all equalities that can be proven are true. The models we are interested in are *algebras*: an algebra is a pair $\langle A, F \rangle$ where A is a set of objects and F is a set of functions such that for any function $f \in F$ with arity n, $f : A^n \rightarrow A$.

A class of algebras is a *variety* if it consists of the models of some (finite or infinite) set of equations. Varieties were characterized by Birkhoff in the following algebraic way: A class of algebras is a variety iff it is closed under Cartesian products, subalgebras, and homomorphic images. That is, a class $\mathcal{K}$ of algebras is a variety if (a) for any $\mathbf{A}_1, \ldots, \mathbf{A}_n$ in $\mathcal{K}$ $(n \geq 0)$, their product $\mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ is also in $\mathcal{K}$, where $f_{\mathbf{A}_1 \times \cdots \times \mathbf{A}_n}(\ldots \langle a_1, \ldots, a_n \rangle \ldots) = \langle f_{\mathbf{A}_1}(\ldots a_1 \ldots), \ldots, f_{\mathbf{A}_n}(\ldots a_n \ldots) \rangle$; (b) for any subset B of A for algebra $\mathbf{A}$ in $\mathcal{K}$, the subalgebra obtained by restricting $f_{\mathbf{A}}$ to B for each f in $\mathcal{F}$ is also in $\mathcal{K}$; and (c) for any homomorphism $\theta : A \rightarrow B$ between universes, if A is in $\mathcal{K}$, then so is the algebra $\mathbf{B}$ wherein $f_{\mathbf{B}}(\ldots a_i\theta \ldots) = f_{\mathbf{A}}(\ldots a_i \ldots)\theta$.

If E is terminating and confluent, we have the following equivalences:

- $\mathcal{M}od(E) \models s = t \Leftrightarrow E \vdash s = t$ according to the completeness theorem
- $E \vdash s = t \Leftrightarrow s \underset{E}{\overset{*}{\leftrightarrow}} t$. Proving equality with the axioms in E is equivalent to the congruence of the two terms using the rewrite version of E.
- $s \underset{E}{\overset{*}{\leftrightarrow}} t \Leftrightarrow s \underset{E}{\overset{*}{\rightarrow}} x \underset{E}{\overset{*}{\leftarrow}} t$ because of the confluence of E
- $s \underset{E}{\overset{*}{\rightarrow}} x \underset{E}{\overset{*}{\leftarrow}} t \Leftrightarrow s \underset{E}{\overset{!}{\rightarrow}} e \underset{E}{\overset{!}{\leftarrow}} t$ where e is a normal form, because of the termination of E

Therefore the semantic notion of $=_E$ is equivalent to the syntactic notion of $\underset{E}{\overset{*}{\leftrightarrow}}$. In other words, two terms are equal iff they have the same normal form.
This equivalence can be used to show that it is not the case that $x + y = y + x$ in our system of addition, because both $x + y$ and $y + x$ are normal forms, and therefore $x + y \underset{E}{\overset{*}{\not\leftrightarrow}} y + x$.

Models of E

Some of the models of E are of special interest.
The trivial model is the model that contains only one object, with all functions mapping onto this object. In this model all equalities hold, because all the terms map to the same object. In this respect, the trivial model can be considered maximal.
The quotient term algebra: There exists, for every set of axioms E, a minimal model as well. This is the model in which exactly those equalities which are true in all models of E hold:
$\exists \mathcal{M}_E$ a model, such that $E \models s = t \Leftrightarrow \mathcal{M}_E \models s = t$
The construction of $\mathcal{M}_E$ is as follows: Take $\mathcal{T}$ and divide it into equivalence classes using the equivalence relation $\underset{E}{\overset{*}{\leftrightarrow}}$. An example for such an equivalence class for our addition axioms, E_a, is
$[s0 + ssz]_E = [s(s0 + sz)]_E = [ss(s0 + z)]_E = [s0 + s(sz + 0)]_E = \ldots.$
The objects of $\mathcal{M}_E$ are these equivalence classes, denoted: $\mathcal{M}_E = \mathcal{T}/E$.
For each functions in $\mathcal{F}$, we define the following interpretation:
$f_{\mathcal{M}_E}([x_1]_E, \ldots, [x_n]_E) \equiv [f(x_1, \ldots, x_n)]_E$.
Since $s = t \Leftrightarrow s \underset{E}{\overset{*}{\leftrightarrow}} t$, we get $\mathcal{T}/E \models s = t \Leftrightarrow \mathcal{M}od(E) \models s = t$.

The Initial algebra: Let us consider the set $\mathcal{G}$ of terms over $\mathcal{F}$ only. The terms in $\mathcal{G}$ are called *ground* terms, or variable-free terms. If we divide $\mathcal{G}$ into equivalence classes over $\overset{*}{\underset{E}{\leftrightarrow}}$, we get the *initial algebra* of E denoted: $\mathcal{I}_E = \mathcal{G}/E$. For example, for our addition axioms, E_a, the equivalence class $[ss(s0 + s0)]_E = [sss0]_E = \ldots$ is an object in the initial algebra. Many equalities hold in the initial algebra that do not hold in the minimal model, $\mathcal{T}/E$. For example, $\mathcal{G}/E_a \models x + y = y + x$. The initial algebra of E_a is exactly the standard model of natural numbers.
As was shown before, since E is Church-Rosser and terminating, $\mathcal{M}od(E) \models s = t \Leftrightarrow \exists e, s \overset{!}{\underset{E}{\rightarrow}} e \overset{!}{\underset{E}{\leftarrow}} t$. Therefore, all the terms in a specific equivalence class have the same normal form. The normal form can be used as a 'natural' representative of the equivalence class. We can define the models $\mathcal{M}_E$ and $\mathcal{I}_E$ as $NF(\mathcal{T})$ and $NF(\mathcal{G})$, respectively, where $NF(X) = \{t \in X | \neg\exists z, z \rightarrow t\}$. This definition is isomorphic to our previous definition with equivalence classes.

Functions and Constructors

When we define a set of axioms that describe the requirements from a program, we usually consider some symbols as functions, having a value for each set of arguments, while other symbols define the objects that we are referring to. For example, in E_a, we had the symbols $s, 0, +$. The symbol $+$ represents a function and we wouldn't want it to be a part of an object's name, and the symbols $s, 0$ define all the objects in $NF(\mathcal{G})$ which is, in our case, the model of natural numbers. We therefore define a division of $\mathcal{F}$, the set of functions over which E is constructed, into two sets: $\mathcal{C}$ is the set of *constructors*, and $\mathcal{D}$ is the set of *defined functions*. The constructors are the symbols that objects are constructed from, while the defined functions are functions we want to be computed. In our example, $\mathcal{C} = \{s, 0\}$ and $\mathcal{D} = \{+\}$.
We would like, for each defined function, to have a value for any set of arguments, that is constructed only of constructors. We will denote the set of ground-constructor-terms $\mathcal{G}_C$.

Definition 1 (Sufficiently Complete) *A function $f \in \mathcal{D}$ of arity n is* sufficiently complete *for E if:*
$\forall s_1, \ldots, s_n \in \mathcal{G}_C, \quad \exists g \in \mathcal{G}_C, \quad f(s_1, \ldots, s_n) =_E g.$

If, for example, we would have left out the rule $x + 0 \rightarrow x$ when defining E, the term $0 + 0$ would have been a normal form, and therefore would have been an object seperate from 0 in $NF(\mathcal{G})$. Therefore, + would not be sufficiently complete.

Using axioms to test program correctness

We have seen that on many cases, when we define a program's requirements with a set of axioms, what we actually want, is not compliance with the most general model (the quotient term algebra) but compliance with the initial algebra. For example, we would like to allow a programmer to add a rule such as $0 + x \rightarrow x$ (e.g. for the purpose of optimizing computation speed) to E_a. This rule is not valid in all models of E_a, but it is valid in the standard model of natural numbers.

Unfortunately, it is not possible in general to prove that a certain rule is valid in the initial algebra, in contrast with the completeness theorem we have for the quotient term algebra.

Many properties of the initial algebra can be proven using induction over some well founded order over the terms. When E is Church-Rosser and terminating, the relaton $\underset{E}{\overset{*}{\rightarrow}}$ is well founded, and therefore can be used as a natural order for induction proofs. The structure of such a proof would be:

To prove $\forall x,\ P(x)$,

prove $\forall x,\ ((\forall y \underset{E}{\overset{*}{\rightarrow}} x, P(y)) \Rightarrow P(x))$.