Formal Methods
6. Algebraic Semantics

Nachum Dershowitz

April 2000

Let $\mathcal{T}$ be all terms constructed from function symbols $\mathcal{F}$ and variables $\mathcal{X}$. Let $\mathcal{G}$ be the *ground* or variable-free terms in $\mathcal{T}$. Terminating and confluent relations are called *convergent* or *complete*. Often, we are only interested in confluence of rewriting for ground terms in $\mathcal{G}$ and speak of *ground convergent* rewrite systems.

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 $\theta : A \to B$ between universes, if A is in $\mathcal{K}$, then so is the algebra $\mathbf{B}$ wherein $f_{\mathbf{B}}(\ldots a_i\theta \ldots) = f_{\mathbf{A}}(\ldots a_i \ldots)\theta$.

The quotient algebra $\mathcal{T}/E$ of equivalence classes of terms in $\mathcal{T}$ is one of the models of E. Since these classes are defined by the congruence $\leftrightarrow^*_E$, which is just replacement of equals, we have $\mathcal{T}/E \models s = t$ implies $E \vdash s = t$. Hence:

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 $\mathcal{T}/E \models s = t$ iff $E \vdash s = t$.*

Accordingly, we may use the semantic notion $=_E$ and syntactic notion $\leftrightarrow^*_E$ interchangeably. It follows that a convergent rewrite system R decides validity for the models of its rules, since $s \leftrightarrow^*_R t$ iff $R(s) = R(t)$.

A substitution is a homomorphism from $\mathcal{T}$ to itself. If there exists a substitution $\sigma : \mathcal{T} \to \mathcal{T}$ such that $s\sigma$ and $t\sigma$ are identical, then for any algebra $\mathbf{B}$ there exists a homomorphism $\theta : \mathcal{T} \to \mathbf{B}$ such that $s\theta = t\theta$. In other words, if an equation is satisfiable in the term algebra $\mathcal{T}$, then it is satisfiable in all algebras. Similarly, any equation satisfiable in the quotient algebra $\mathcal{T}/E$ is satisfiable in all algebras in $\mathcal{M}od(E)$. (Satisfiability in $\mathcal{T}$ is called *unifiability*.)

For many purposes, not all models are of equal interest. One generally asks whether an equation is valid in a specific model. (Of course, all equations are valid, let alone satisfiable, in a trivial algebra having only one element in its universe.) For applications like abstract data types, attention is often focused on those "standard" models that are (finitely) generated from the signature itself, in which every element of the universe is the interpretation of some term.

An algebra $\mathbf{A}$ in a class $\mathcal{K}$ of algebras is *free* over a set $\mathcal{X}$ of variables if $\mathcal{X}$ is a subset of A and, for any algebra $\mathbf{B} \in \mathcal{K}$ and assignment $\theta : \mathcal{X} \to B$, there exists a unique homomorphism $\phi : \mathbf{A} \to \mathbf{B}$ such that ϕ and θ agree on $\mathcal{X}$. A free algebra is unique up to isomorphism, whenever it exists. The *(absolutely)* free algebra over $\mathcal{X}$ among all algebras is just (isomorphic to) the *term algebra* $\mathcal{T}(\mathcal{F}, \mathcal{X})$ with the the symbol $f \in \mathcal{F}$ itself as the operator $f_{\mathcal{T}}$. An algebra $\mathbf{A}$ in a class $\mathcal{K}$ of algebras is *initial* if, for any algebra $\mathbf{B}$ in $\mathcal{K}$ there exists a unique homomorphism $\phi : \mathbf{A} \to \mathbf{B}$. The initial object among all $\mathcal{F}$-algebras is (isomorphic to) the *ground-term algebra* $\mathcal{G}(\mathcal{F})$, again with the function symbol itself as operator, and corresponds to the Herbrand universe over the symbols in $\mathcal{F}$. The importance of the initial algebra lies in its uniqueness (it is the free algebra for empty $\mathcal{X}$), and in the fact that the class $\mathcal{K}$ consists of its homomorphic images, making it the most "abstract" amongst them.

Among all models of a set of equations E, the prototypical one is the initial algebra $\mathcal{I}(E)$ of E. Its universe consists of one element for each E-congruence class of ground terms. In other words, $\mathcal{I}(E)$ is (isomorphic to) the quotient $\mathcal{G}/E$ of the ground-term algebra $\mathcal{G}$ and the congruence $\leftrightarrow^*_E$ (restricted to $\mathcal{G}$). This algebra can be realized if R is a ground convergent rewrite system for E, since, then, E-equivalent ground terms have the same R-normal form. Accordingly, the *normal-form algebra* of R has the set of ground R-normal forms as its universe and operations f_R defined by $f_R(t_1, \ldots, t_n) = R(f(t_1, \ldots, t_n))$ for all normal forms t_i. This algebra is (isomorphic to) the initial algebra $I(R)$ of the variety defined by the rules in R

considered as equations. Thus, rewriting computes ground normal forms that are representatives of their congruence classes. It is in this sense that rewriting is a "correct" implementation of initial-algebra semantics. Specification languages based on abstract data types, follow this implementation scheme: equations are used as rewrite rules, and unique normalization is needed for the operational and initial-algebra semantics to coincide.

Exactly those variable-free equations that follow necessarily from E hold in the initial algebra. Thus, the word problem for E, i.e. deciding, for *ground* terms s and t, whether $s = t$ holds in every model of E, is the same as determining if $\mathcal{I}(E) \models s = t$. More generally, one may ask if an equation $s = t$ (possibly containing variables) is valid in the initial algebra $\mathcal{I}(E)$, which is the case iff all of its ground instances hold for $\mathcal{M}od(E)$. The class $\mathcal{I}nd(E)$ of equations valid in $\mathcal{I}(E)$is called the *inductive theory* of E. Unlike equational theories, inductive theories are not necessarily recursively enumerable (even for finite E).