**Mathematical Semantics of Computer Systems, *MSCS* (4810-1168)**
**Handout for Lecture 10 (2015/01/05)**

Ichiro Hasuo, Dept. Computer Science, Univ. Tokyo  `http://www-mmm.is.s.u-tokyo.ac.jp/~ichiro`

Remember: we loosely follow [4], but it hardly serves as an introductory textbook. More beginner-friendly ones include [1, 5]; other classical textbooks include [6, 2]. nLab (`ncatlab.org`) is an excellent online information source.

# 1 On the Yoneda Lemma (Ctn'd)

- Cayley's representation theorem (recap)
- Generalizing a group (hence a monoid) to a category: an arrow becomes a function. How?
  - Answer:

$$\dfrac{\dfrac{X \longrightarrow X' \text{ in } \mathbb{C}}{\mathbb{C}(\_\,, X) \Longrightarrow \mathbb{C}(\_\,, X'),\ \text{nat. trans.}}\ \text{(the Yoneda lemma)}}{\mathbb{C}(Y, X) \longrightarrow \mathbb{C}(Y, X'),\ \text{one function for each } Y\text{; natural in } Y}$$

- The Yoneda embedding $\mathbf{y}$ carries $X \in \mathbb{C}$ to a presheaf $\mathbf{y}X = \mathbb{C}(\_\,, X)$
  - A basic idea in category theory: the identity of objects do not matter; what matters is how an object is "related" to others
  - The Yoneda embedding $\mathbf{y}$ gives an abstract representation of an object $X$ as "a guy to which another object $Y$ has the set $\mathbb{C}(Y, X)$ of arrows"
  - Listing up some guy's properties identifies the guy!
- Proof of the lemma that John proved in concrete terms:

  a left adjoint, if it exists, is unique up-to natural isomorphisms

**Lemma.** *Homfunctors preserve (co)limits.*

# 2 Algebraic Semantics as a Precursor of Categorical Semantics

This section is essentially a brief recap of [3, Chap. 2], aimed also at the audience not familiar with formal logic.

## 2.1 The Word Problem

Consider the following "syntactic system."

- *Terms* are defined by the following BNF notation:

$$\textbf{Terms} \ni t, t_1, t_2 \quad ::= \quad \mathtt{x} \in \textbf{Var} \mid \mathtt{e} \mid t \cdot t \mid t^{-1} \ .$$

- The relation $\sim$ between terms is defined inductively by the following rules.

$$\frac{}{(t_1 \cdot t_2) \cdot t_3 \sim t_1 \cdot (t_2 \cdot t_3)}\ (\textsc{Associativity})$$

$$\frac{}{\mathsf{e} \cdot t \sim t}\ (\textsc{Unit-Left}) \qquad \frac{}{t \cdot \mathsf{e} \sim t}\ (\textsc{Unit-Right})$$

$$\frac{}{t^{-1} \cdot t \sim \mathsf{e}}\ (\textsc{Inverse-Left}) \qquad \frac{}{t \cdot t^{-1} \sim \mathsf{e}}\ (\textsc{Inverse-Right})$$

$$\frac{}{t \sim t}\ (\textsc{Reflexivity}) \qquad \frac{t \sim s}{s \sim t}\ (\textsc{Symmetry}) \qquad \frac{t \sim s \quad s \sim u}{t \sim u}\ (\textsc{Transitivity})$$

$$\frac{t_1 \sim s_1 \quad t_2 \sim s_2}{t_1 \cdot t_2 \sim s_1 \cdot s_2}\ (\cdot\text{-}\textsc{Congruence}) \qquad \frac{t \sim s}{t^{-1} \sim s^{-1}}\ ((\_)^{-1}\text{-}\textsc{Congruence})$$

**Remark.** (For those who are *not* familiar with formal logic) The "inductive definition of $\sim$ by the rules" means that we have $t \sim s$ if and only if we can draw a (finite-height) *proof tree* using the rules, for example

$$\dfrac{\dfrac{}{((xy)^{-1}x)y \sim (xy)^{-1}(xy)}\ (\textsc{Associativity}) \quad \dfrac{}{(xy)^{-1}(xy) \sim e}\ (\textsc{Inverse-Left})}{((xy)^{-1}x)y \sim e}\ (\textsc{Transitivity})$$

**Remark.** (For those who *are* familiar with formal logic) The above is an equational theory of groups, formulated as usual in equational logic.

Now the question is: given terms $s$ and $t$, can we know if $s \sim t$ holds? How? This problem is known as the *word problem for groups.*

**Theorem** (Novikov, 1955)**.** *The word problem for groups is undecidable.*

Therefore there is no generic algorithm that decides the problem.

## 2.2 Use of Algebraic Semantics

For those of you who are familiar with abstract algebra or group theory, the following fact will come as trivial.

> (†) If there is a group $G$ in which the terms $s$ and $t$ are not equal, then we know that $s \sim t$ does not hold.

Implicit here is the use of *algebraic semantics.*

**Definition.** Let $G$ be a group and $V\colon \mathbf{Var} \to |G|$ be a function (here $|G|$ denotes the underlying set of $G$; we call the function $V$ a *valuation*). The *denotation* $[\![t]\!]_V$ of a term $t$ under $V$ is an element of the group $G$ defined in the obvious inductive way; namely

$$[\![x]\!]_V := V(x) \qquad [\![\mathsf{e}]\!]_V := e_G$$
$$[\![t_1 \cdot t_2]\!]_V := [\![t_1]\!]_V \cdot_G [\![t_2]\!]_V \qquad [\![t^{-1}]\!]_V := \bigl([\![t]\!]_V\bigr)^{-1} .$$

Note here that the unit, the multiplication operator and the inverse operator on the left-hand sides are syntactic symbols; those on the right-hand sides are mathematical/semantical operators in the group $G$.

Now it is possible to "investigate" whether $s \sim t$ holds by looking at their semantics.

**Theorem** (soundness)**.** *If $s \sim t$ holds, then $[\![s]\!]_V = [\![t]\!]_V$ for any group $G$ and any valuation $V : \mathbf{Var} \to |G|$.*

*Proof.* Straightforward, by structural induction on the construction of proof trees. □

You see that the quotation (†) in the above is the (sloppily stated version of the) contraposition of the theorem. Therefore, to *refute* $s \sim t$, it suffices to find convenient $G$ and $V$ such that $[\![s]\!]_V \neq [\![t]\!]_V$.

## 2.3 Completeness and the Term Model

The obvious question that remains is: is the above "investigation method" complete, too? The answer is positive:

**Theorem** (completeness)**.** *Assume that $[\![s]\!]_V = [\![t]\!]_V$ for any group $G$ and any valuation $V : \mathbf{Var} \to |G|$. Then $s \sim t$ holds.*

*Proof.* We can in fact construct a special group $G_0$ by syntactic means—and a special valuation $V_0 : \mathbf{Var} \to |G_0|$ that accompanies—such that $[\![s]\!]_{V_0} = [\![t]\!]_{V_0}$ if and only if $s \sim t$ holds.

Concretely:

- $|G_0| = \{ [s]_\sim \mid s \text{ is a term} \}$, where $[s]_\sim$ is the $\sim$-equivalence class of the term $s$
- Operations are defined syntactically, that is for example,

$$[s]_\sim \cdot_{G_0} [t]_\sim \;=\; [s \cdot t]_\sim \tag{1}$$

  and so on. Note here that $\cdot_{G_0}$ on the left-hand side is a semantical/mathematical entity (a group multiplication); in contrast $\cdot$ on the right-hand side is a syntactic entity (an operation symbol).

We have to check the following. These are all straightforward.

- $\sim$ is an equivalence relation of terms. (This follows from the rules that define $\sim$)
- The operations in (1) are well-defined. (Follows from the Congruence rules)
- The set $|G_0|$, together with the operations defined as in (1), forms a group. (Easy)

We define the valuation $V_0$ by

$$V_0(x) \;:=\; [x]_\sim \;. \tag{2}$$

Then it is straightforward by induction to show that $[\![s]\!]_{V_0} = [s]_\sim$. This establishes: $[\![s]\!]_{V_0} = [\![t]\!]_{V_0}$ if and only if $s \sim t$. □

The group $G_0$ that we constructed is often called a *term model*, since it consists of (equivalence classes of) terms. A term model is a complete model—in the sense that $[\![s]\!]_{V_0} = [\![t]\!]_{V_0}$ if and only if $s \sim t$—but a common problem with it is that equality in the term model is complicated (deciding it is as hard as deciding $\sim$ itself!).

The term model $G_0$, in the current setting of an algebraic theory for groups, turns out to be isomorphic to the *free group* over the set **Var** of generators. It is called a *free* group since it satisfies the minimal set of equalities for it to be a group, in the sense that

$[\![s]\!]_{V_0} = [\![t]\!]_{V_0}$ if and only if $s \sim t$.

## References


[1] S. Awodey. *Category Theory*. Oxford Logic Guides. Oxford Univ. Press, 2006.

[2] M. Barr and C. Wells. *Toposes, Triples and Theories*. Springer, Berlin, 1985. Available online.

[3] I. Hasuo. Introduction to logic and computability. Course material for the undergraduate course *Information Logic*, 2014. Available on the web, `www-mmm.is.s.u-tokyo.ac.jp/~ichiro/courseNotes/textbookInfLogic.pdf` (restricted access from inside UTokyo).

[4] J. Lambek and P.J. Scott. *Introduction to higher order Categorical Logic*. No. 7 in Cambridge Studies in Advanced Mathematics. Cambridge Univ. Press, 1986.

[5] T. Leinster. *Basic Category Theory*. Cambridge Univ. Press, 2014.

[6] S. Mac Lane. *Categories for the Working Mathematician*. Springer, Berlin, 2nd edn., 1998.