Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 319 (2015) 255–270

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Healthiness Conditions for Predicate Transformers

Klaus Keimel [1,2]

Fachbereich Mathematik
Technische Universität Darmstadt
64289 Darmstadt, Germany

Abstract

The behavior of a program can be modeled by describing how it transforms input states to output states, the *state transformer semantics*. Alternatively, for verification purposes one is interested in a 'predicate transformer semantics' which, for every condition on the output, yields the weakest precondition on the input that guarantees the desired property for the output.

In the presence of computational effects like nondeterministic or probabilistic choice, a computation will be modeled by a map $t\colon X \to \mathcal{T}Y$, where $\mathcal{T}$ is an appropriate computational monad. The corresponding predicate transformer assigns predicates on Y to predicates on X. One looks for necessary and, if possible, sufficient conditions (healthiness conditions) on predicate transformers that correspond to state transformers $t\colon X \to \mathcal{T}Y$.

In this paper we propose a framework for establishing healthiness conditions for predicate transformers. As far as the author knows, it fits to almost all situations in which healthiness conditions for predicate transformers have been worked out. It may serve as a guideline for finding new results; but it also shows quite narrow limitations.

Keywords: predicate transformers, healthiness conditions, continuation monad, commuting operations, entropic algebras

1 Introduction: An example

In denotational semantics we distinguish two complementary approaches that we shortly call state transformer semantics and predicate transformer semantics. Let us begin with the well-known example of angelic nondeterminism to explain our intentions. As semantic domains we will use directed complete partially ordered sets (dcpos), maps will be Scott-continuous, that is, they preserve the order and suprema of directed subsets.

In the presence of nondeterministic choice, running a program for an input x belonging to a domain X will lead to a set $t(x)$ of possible outputs in a domain Y. In

[1] Supported by Deutsche Forschungsgemeinschaft

[2] Email: keimel@mathematik.tu-darmstadt.de

http://dx.doi.org/10.1016/j.entcs.2015.12.016

1571-0661/© 2015 The Author. Published by Elsevier B.V.

the angelic interpretation of nondeterminism, $t(x)$ will be a non-empty Scott-closed subset of the dcpo Y and t will be a Scott-continuous map from the dcpo X to the *Hoare powerdomain* $\mathcal{H}Y$ of all nonempty Scott-closed subsets of Y. The binary choice operator is interpreted by union on the Hoare powerdomain. Thus, a program will be interpreted by a *state transformer*, a Scott-continuous map $t: X \to \mathcal{H}Y$.

Observable predicates on Y are Scott-open subsets U of Y (see, e.g., [25]). Thus, the complete lattice $\mathcal{O}Y$ of all Scott-open subsets of Y represents the dcpo of predicates on Y. A Scott-continuous map $p: \mathcal{O}Y \to \mathcal{O}X$ transforming predicates on Y to predicates on X will be a *predicate transformer*.

To a state transformer $t: X \to \mathcal{H}Y$ we associate the predicate transformer $p: \mathcal{O}Y \to \mathcal{O}X$ defined by:

$$p(U) = \{x \in X \mid t(x) \cap U \neq \emptyset\}$$

the set of all points in X that lead to at least one output with the desired property U (the angelic point of view). The state transformer t can be recovered from the associated predicate transformer p by

$$t(x) = \bigcap \{Y \setminus U \mid x \notin p(U)\}$$

We are concerned with the problem to find properties (healthiness conditions) that characterize those predicate transformers $p: \mathcal{O}Y \to \mathcal{O}X$ that correspond to state transformers $t: X \to \mathcal{H}Y$. The answer in this case is:

The predicate transformers $p: \mathcal{O}Y \to \mathcal{O}X$ that correspond to state transformers $t: X \to \mathcal{H}Y$ are characterized by the properties:

$$p(\emptyset) = \emptyset, \quad p(U \cup U') = p(U) \cup p(U')$$

Equivalently, these are the maps p preserving arbitrary unions.

The above considerations become more elegant, but less intuitive, by passing to a functional setting. We use that the category DCPO of dcpos and Scott-continuous maps is Cartesian closed. The exponential of two dcpos X and Y,

$$\text{denoted by } Y^X \text{ and equally by } [X \to Y]$$

is the dcpo of all Scott-continuous maps $u: X \to Y$ with the pointwise defined order (one may consult [3] for background on dcpos).

We endow the two element domain $\mathbf{2} = \{0 < 1\}$ with the structure of a unital semilattice with $x \vee y = \max(x, y)$ and the constant (unit) 0. A predicate (a Scott-open subset U) of a dcpo Y is identified with the Scott-continuous map $f_U: Y \to \mathbf{2}$ with value 1 iff $x \in U$. Thus the dcpo $\mathcal{O}Y$ of predicates is identified with the function space $\mathbf{2}^Y$. This function space is also a unital semilattice when equipped with the pointwise defined operation $\vee$ and the constant function 0. The Scott-continuous unital semilattice homomorphisms $\varphi: \mathbf{2}^Y \to \mathbf{2}$ form a dcpo $[\mathbf{2}^Y \xrightarrow{\vee,0} \mathbf{2}]$ which is also a unital semilattice for the pointwise defined semilattice operations. We will use that it is isomorphic to the Hoare powerdomain $\mathcal{H}Y$; indeed, these homomorphisms φ correspond to the Scott-closed subsets of Y by assigning to φ the Scott-closed set $C = Y \setminus \bigcup \{U \in \mathcal{O}Y \mid \varphi(f_U) = 0\}$.

Now a state transformer will be a Scott-continuous map $t: X \to [\mathbf{2}^Y \xrightarrow{\vee,0} \mathbf{2}]$ and a