GAME SEMANTICS

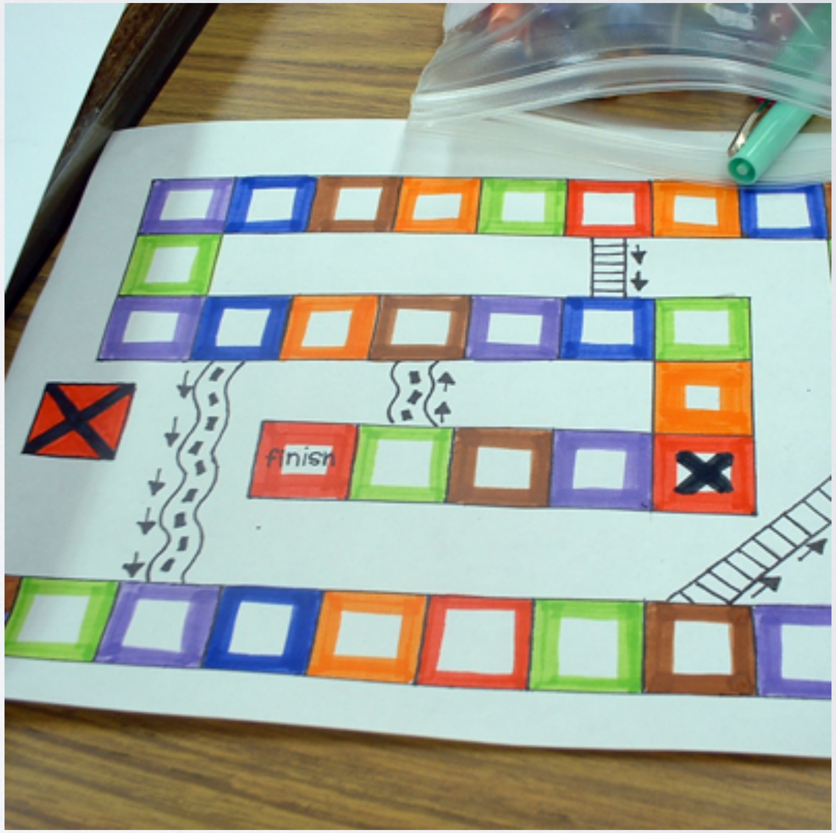
Andrzej Murawski
UNIVERSITY OF OXFORD

Nikos Tzevelekos
QUEEN MARY
UNIVERSITY OF LONDON

DISCLAIMERS

- computer games
- game theory
- games logicians play
- parity games

OLYMPIC SPIRIT



TOWARD A MATHEMATICAL SEMANTICS FOR COMPUTER LANGUAGES

this passage. The purpose of a mathematical semantics is to give a correct and meaningful correspondence between programs and mathematical entities in a way that is entirely independent of an implementation. This plan is illustrated in a very elementary

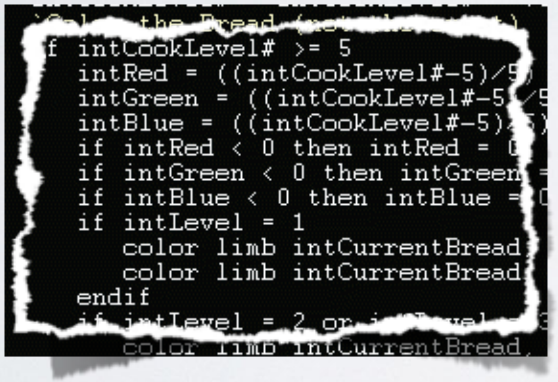
Dana Scott

and

Christopher Strachey

Oxford University
Computing Laboratory
Programming Research Group-Library
8-11 Keble Road
Oxford OX1 3QD
Oxford (0865) 54141

MATHEMATICAL SEMANTICS



$[\![M]\!]$

function

continuous function

strategy

PCF (Scott/Milner/Plotkin)

- Programming Computable Functions
- Prototypical purely functional language
- Features integer arithmetic, higher-order functions and recursion
- Inspired early research on semantics

PCF TYPES

$$\theta \ ::= \ \mathsf{int} \mid \theta \to \theta$$

PCF TERMS

$$
\begin{aligned}
M \quad ::= \; & i \mid x \\
& \mid M \oplus M \mid \textsf{if } M \textsf{ then } M \textsf{ else } M \\
& \mid \lambda x^{\theta}.M \mid M\,M \mid \textsf{div}_{\theta}
\end{aligned}
$$

TYPING JUDGMENTS

$$x_1 : \theta_1, \cdots, x_n : \theta_n \vdash M : \theta$$

PCF TYPING JUDGMENTS

$$\frac{i \in \mathbb{Z}}{\Gamma \vdash i : \mathsf{int}} \qquad \frac{(x : \theta) \in \Gamma}{\Gamma \vdash x : \theta}$$

$$\frac{\Gamma \vdash M : \mathsf{int} \quad \Gamma \vdash N : \mathsf{int}}{\Gamma \vdash M \oplus N : \mathsf{int}} \qquad \frac{\Gamma \vdash M : \mathsf{int} \quad \Gamma \vdash N_0 : \theta \quad \Gamma \vdash N_1 : \theta}{\Gamma \vdash \mathsf{if}\ M\ \mathsf{then}\ N_1\ \mathsf{else}\ N_0 : \theta}$$

$$\frac{\Gamma \uplus \{\, x : \theta \,\} \vdash M : \theta'}{\Gamma \vdash \lambda x^{\theta}.M : \theta \to \theta'} \qquad \frac{\Gamma \vdash M : \theta \to \theta' \quad \Gamma \vdash N : \theta}{\Gamma \vdash MN : \theta'}$$

$$\frac{}{\Gamma \vdash \mathsf{div}_{\theta} : \theta}$$

TOWARDS MEANINGFUL CORRESPONDENCES

- Operational semantics is a compulsory element of a formal definition of a programming language.

$$M \longrightarrow M'$$

- We shall focus on several meaningful correspondences between mathematical and operational semantics.

REDUCTION

$$\begin{array}{rcll} i \oplus j & \longrightarrow & k & (k = i \oplus j) \\ \text{if } 0 \text{ then } M \text{ else } M' & \longrightarrow & M' & \\ \text{if } i \text{ then } M \text{ else } M' & \longrightarrow & M & (i \neq 0) \\ (\lambda x.M)N & \longrightarrow & M[N/x] & \end{array}$$

$$\frac{M \longrightarrow M'}{E[M] \longrightarrow E[M']}$$

$$E ::= [\,] \mid E \oplus M \mid i \oplus E \mid \text{if } E \text{ then } M \text{ else } M \mid EM$$

1. CORRECTNESS

$$\text{If } M \longrightarrow M' \text{ then } [\![M]\!] = [\![M']\!].$$

In particular, if $\vdash M : \mathsf{int}$ and $M \longrightarrow i$ then $[\![M]\!] = [\![i]\!]$.

2. ADEQUACY

The following converse would be too strong:

$$\text{if } [\![M]\!] = [\![M']\!] \text{ then } M \longrightarrow M'.$$

Instead one aims for:

$$\text{Given } \vdash M : \mathsf{int}, \text{ if } [\![M]\!] = [\![i]\!] \text{ then } M \longrightarrow i.$$

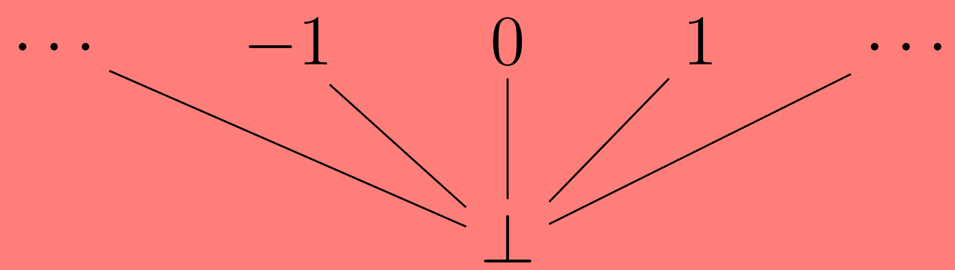
3. DEFINABILITY (NO JUNK)

Suppose $[\![\theta]\!]$ is the mathematical object corresponding to θ, i.e. terms $[\![\vdash M : \theta]\!]$ can be thought of as elements of $[\![\theta]\!]$.

$$\forall_{x \in [\![\theta]\!]} \quad \exists_{\vdash M_x : \theta} \quad x = [\![\vdash M_x : \theta]\!]$$

DOMAIN-THEORETIC SEMANTICS

- Plotkin's domain-theoretic model of PCF uses the following partial order to model **int**.



- Terms are interpreted by monotone functions.
- The model is correct and adequate, but does not have the definability property.

FAILURE OF DEFINABILITY

Consider the **parallel-or** function

$$por\,x\,y = \begin{cases} 0 & x = 0 \text{ and } y = 0 \\ 1 & x \neq 0, \bot \text{ or } y \neq 0, \bot \\ \bot & \text{otherwise} \end{cases}$$

E.g. $por\,0\,0 = 0$ and $por\,1\,\bot = por\,\bot\,1 = 1$.

por turns out to be undefinable:
there is no PCF term M such that

$$M\ \mathsf{div}\ 1 \longrightarrow 1 \qquad M\ 1\ \mathsf{div} \longrightarrow 1 \qquad M\ 0\ 0 \longrightarrow 0$$

TOWARDS FULL ABSTRACTION

$$[\![M_1]\!] = [\![M_2]\!]?$$

CONTEXTUAL TESTING

- Contexts

$$\begin{aligned} C \ ::= & \ [\,] \mid C \oplus M \mid M \oplus C \\ & \mid \textsf{if}\ C\ \textsf{then}\ M\ \textsf{else}\ M \mid \textsf{if}\ M\ \textsf{then}\ C\ \textsf{else}\ M \mid \textsf{if}\ M\ \textsf{then}\ M\ \textsf{else}\ C \\ & \mid \lambda x^{\theta}.C \mid MC \mid CM \end{aligned}$$

- Testing of $M : \theta$

$$C[M] : \textsf{int}$$

If there exists i such that $C[M] \longrightarrow^{*} i$, we write $C[M] \Downarrow$ (success!).

CONTEXTUAL EQUIVALENCE

Intuitively, two programs should be viewed as equivalent if they behave in the same way in any context, i.e. they can be used interchangeably.

- $\Gamma \vdash M_1 : \theta$ ***approximates*** $\Gamma \vdash M_2 : \theta$ if

  $$C[M_1]\Downarrow \text{ implies } C[M_2]\Downarrow$$

  for any context C such that $\vdash C[M_1], C[M_2] : \mathsf{int}$. Then we write $\Gamma \vdash M_1 \sqsubseteq M_2$.

- Two terms are ***equivalent*** if one approximates the other, written $\Gamma \vdash M_1 \cong M_2$.

4. FULL ABSTRACTION

$$[\![M_1]\!] = [\![M_2]\!] \quad \text{if and only if} \quad M_1 \cong M_2$$

Robin Milner (1977)

SOUNDNESS

Correctness and adequacy turn out to imply:

$$\text{if } [\![M_1]\!] = [\![M_2]\!] \text{ then } M_1 \cong M_2.$$

Assume $[\![M_1]\!] = [\![M_2]\!]$ and suppose $M_1 \ncong M_2$, i.e. $C[M_1] \Downarrow$ and $C[M_2] \not\Downarrow$ for some context C (or $C[M_2] \Downarrow$ and $C[M_1] \not\Downarrow$).

- Correctness implies $[\![C[M_1]]\!] = [\![i]\!]$ for some i.
- Adequacy implies $[\![C[M_2]]\!] \neq [\![i]\!]$ for any i.

This is a contradiction, because $[\![M_1]\!] = [\![M_2]\!]$ implies $[\![C[M_1]]\!] = [\![C[M_2]]\!]$ by compositionality.

NO FULL ABSTRACTION

(FOR THE DOMAIN-THEORETIC MODEL)

$$
\begin{aligned}
M_1 \equiv \;\; \lambda f^{\mathsf{int}\to\mathsf{int}\to\mathsf{int}}. \;\; & \mathsf{if}\ (f\ 1\ \mathsf{div})\ \mathsf{then} \\
& \quad (\mathsf{if}\ (f\ \mathsf{div}\ 1)\ \mathsf{then} \\
& \quad\quad (\mathsf{if}\ (f\ 0\ 0)\ \mathsf{then\ div\ else}\ 1) \\
& \quad\quad\quad \mathsf{else\ div}) \\
& \quad\quad \mathsf{else\ div}
\end{aligned}
$$

$$
M_2 \equiv \;\; \lambda f^{\mathsf{int}\to\mathsf{int}\to\mathsf{int}}. \;\; \mathsf{div}
$$

- Because *por* is not definable, we have $M_1 \cong M_2$.
- $[\![M_1]\!](por) \neq [\![M_2]\!](por)$, so $[\![M_1]\!] \neq [\![M_2]\!]$.

INTRINSIC QUOTIENT

In the presence of definability (as well as correctness and adequacy) one can construct fully abstract models by quotienting.

This boils down to recasting the idea of contextual testing inside the model.

Given $x_1, x_2 \in [\![\theta]\!]$,

$$x_1 \sim x_2 \iff \text{“}\forall_{y \in [\![\theta \to \mathsf{int}]\!]} y(x_1) = y(x_2)\text{”}.$$

Then $[\![\cdots]\!]/\sim$ is fully abstract.

This kind of quotienting may be an obstacle in reasoning about equivalence, so one should attempt to find more direct characterizations.

The 2017 Alonzo Church Award

SIGLOG is delighted to announce that the 2017 Church Award goes to 6 people: Samson Abramsky, Martin Hyland, Radha Jagadeesan, Pasquale Malacaria, Hanno Nickau and Luke Ong for [Quoting from the official citation] “providing a fully-abstract semantics for higher-order computation through the introduction of games models, thereby fundamentally revolutionising the field of programming language semantics, and for the applied impact of these models.”