Guidelines

for Formal Specification and Verification

Răzvan Diaconescu

Institutul de Matematică “Simion Stoilow” al Academiei Române

2nd RO-JP AlgSpec Workshop, Sinaia, March 2011

Outline

1. The foundational level

2. The methodological level

3. The ethical level

FOUNDATIONS

SEMANTICS COMES FIRST!

Famous slogan of Joseph Goguen, must be understood through reason.

Current trend to neglect semantics, mostly because of intelectual incapacity.

Absence of formal semantics

=> things interpreted arbitrarily and not uniformly

=> *in-formal* method

=> non-sense concept of correctness.

Mathematical foundations

- There is a formal logical system, including both model theory (for semantics) and proof theory. Very desirable that these constitute an *institution*.
- The institution has additional structure and enjoys the properties supporting specification in-the-small and in-the-large.
- The eventual operational level of the proof theory (e.g. rewriting) is rigorously supported by mathematics.

Formal specification

- There is a formal specification language such that the language constructs correspond exactly to mathematical entities in the underlying logic.
- A specification consists of
  - a set of *axioms* in the underlying logic (this includes the specification of a corresponding signature), and
  - eventually, structuring constructs.
- Each such specification defines the *class of models* satisfying its axioms.
  - In the structured case, this is also determined by the structuring constructs (requires a bit of mathematical sophistication).

The whole point of formal specification:

axiomatic definition of certain classes of models.

Formal verification via Proof score programming

- Specification of the proof structure, including lemmas, conditions, proof tasks to be executed by the system, etc.
- Should be rigorously, directly and *transparently* based upon mathematical results lying foundations to corresponding proof methodologies.
  - In particular, this means to avoid abuse or even any use of extra-logical features of the language (such as ==, etc.)

Institutional structure and properties

Necessary for proper functioning of the specification language:

- Signature pushouts (co-limits)
- Model amalgamation
- Inclusion systems for signatures
- Free models (for initial semantics)
- Interpolation

Signature pushouts

$$\begin{tikzcd}
\Sigma \arrow[r, "\varphi_1"] \arrow[d, "\varphi_2"'] & \Sigma_1 \arrow[d, "\theta_1"'] \arrow[rdd, bend left, "f_1"] & \\
\Sigma_2 \arrow[r, "\theta_2"] \arrow[rrd, bend right, "f_2"'] & \Sigma' \arrow[rd, "f'"] & \\
 & & \Omega
\end{tikzcd}$$

Model amalgamation

$\mathscr{I}$ *has model amalgamation* when for each pushout of signature morphisms

$$\begin{tikzcd}
M & & & M_1 \\
& \Sigma \arrow[r, "\varphi"] \arrow[d, "\theta"'] & \Sigma_1 \arrow[d, "\theta'"] & \\
& \Sigma_2 \arrow[r, "\varphi'"'] & \Sigma' & \\
M_2 & & & M'
\end{tikzcd}$$

for any Σ_i models M_i such that $\mathrm{M{\small OD}}(\varphi)(M_1) = \mathrm{M{\small OD}}(\theta)(M_2)$

there exists an unique Σ'-model M' such that

$\mathrm{M{\small OD}}(\theta')(M') = M_1$ and $\mathrm{M{\small OD}}(\varphi')(M') = M_2$.

Other useful forms of model amalgamation

Each of the following has its own applications.

- *Weak amalgmation*: requires only the existence of amalgamation M', not uniqueness. Quite often this is sufficient (such as for establising the Satisfaction Condition for quantifiers).
- *Semi-exactness*: amalgamation of model homomorphisms too.
- *J-amalgamation*: amalgamation from J-co-limits rather than just pushuts.

Inclusion systems

- Capture abstractly the concept of set-theoretic inclusion $A \subseteq B$.
- They constitute an alternative for the famous categorical concept of *factorization systems*.
- Signature inclusions, very necessary for the semantics of structured specifications.
- But also good applications to (categorical, institution-independent) model theory.

Inclusion systems: definition

$(\mathscr{I},\mathscr{E})$ is a *inclusion system* for a category $\mathbb{C}$ if

- $\mathscr{I}$ (*abstract inclusions*) and
- $\mathscr{E}$ (*abstract surjections*)

are two sub-categories such that

1. $|\mathscr{I}| = |\mathscr{E}| = |\mathbb{C}|$
2. $\mathscr{I}$ is a partial order ($\subseteq$), and
3. every arrow f in $\mathbb{C}$ can be factored uniquely as

$$\begin{tikzcd} A \arrow[r, "e_f \in \mathscr{E}"] \arrow[rr, bend right, "f"'] & B \arrow[r, "i_f \in \mathscr{I}"] & C \end{tikzcd}$$

Properties of inclusiom systems

- It has $\cup$ and $\cap$.
- It is epic.
- It admits free idempotent extensions along signature inclusions.

$(\mathscr{L},\mathscr{R})$-Interpolation

For signature pushout:

$$\begin{tikzcd}
\Sigma \arrow[r, "\varphi\in\mathscr{L}"] \arrow[d, "\theta\in\mathscr{R}"'] & \Sigma_1 \arrow[d, "\theta'"] \\
\Sigma_2 \arrow[r, "\varphi'"'] & \Sigma'
\end{tikzcd}$$

for $E_i \subseteq Sen(\Sigma_i)$ if $\theta'(E_1) \models_{\Sigma'} \varphi'(E_2)$
then there exists $E \subseteq Sen(\Sigma)$ such that

- $E_1 \models_{\Sigma_1} \varphi(E)$ and
- $\theta(E) \models_{\Sigma_2} E_2$.

METHODOLOGIES

Methodologies

Vast topic.

Language without companion methodologies is un-usable.

One language - several methodologies.

Can methodologies support the usage of formal specification language without proper understanding of formal semantics?

ETHICS

Rapid deterioration of the academic environments

- Based upon competition for power and status.
- De-humanized.
- Critical moment to stop and reverse the trend, later may be too late.

What is wrong with (academic) Power/Status?

They are both evil since:

- ruthless competition to achieve them
- and even more to maintain them.

What is wrong with Competition?

(Academic) competition leads to fraud and exploitation.

- Authors by status often without understanding their authored papers.
- Students/junior researchers as means to achieve funding and research agendas.
- Conferences as platforms of self promotion, interest in other people work only for developing criticism.
- Plagiarism.

What is wrong with Intelectual Property?

- Heavily unrealistic, everything in the intelectual realm inter-dependent with a myriad of other things.
- Self grasping of ideas; similar to how animals mark their teritory.
- Plagiarism as an extreme form of intelectual property grasping; similar to how animals mark *others* teritory.

Solutions

- Refrain as much as possible from co-authorship with own students or junior researchers authors, or at least
- treat them as equal work partners if not as more important then ourselves.
- Regular single authorship, take responsibility to fulfill own research agendas by ourselves (like all great scientists have done in the past, e.g. Newton, Gauss, Einstein, Gödel, Turing, Kripke, etc.)
- Serve the development of our juniors free of own (research or competition) agendas; similar to good parenthood.
- Read more write less.
- Slow down.
- Do all these as a *satyagraha*.