On the justification of formal methods

Roger Bishop Jones

ICL Defence Systems
This document consists of the overheads for a presentation at
the FST quarterly meeting at ICL Winnersh on 16th January 1991.

on

THE JUSTIFICATION

of

FORMAL METHODS

Why do we care?

What kind of enterprise is it?

What kinds of justification are there?

Which justifications hold water?

WHY DO WE CARE?

- **methods work**

  we are consulted on methods and have to present some arguments in favour of specific methodological proposals

- **broadening of customer base**

  we are developing tools and will need to broaden our customer base to justify sustained development of these tools

- **professional standards**

  our reputation depends upon our self critical attitude to our work, this attitude must continue to apply to methods

- **consistency with tool standards**

  we have taken particular care over the integrity and soundness of our proof tools; this is worthless unless we have confidence in the methods which they support

METHODS
are the
WEAKEST LINK

FOUNDATIONAL PROBLEMS are MARGINAL

TOOL INTEGRITY PROBLEMS are SOLUBLE

TOOL PRODUCTIVITY PROBLEMS
are
NOT A SOURCE OF UNSOUNDNESS

METHODOLOGICAL PROBLEMS are SERIOUS

the EASIEST WAY to FAKE VERIFICATION is:
PROVE AN IRRELEVANT PROPOSITION

WHAT KIND OF ENTERPRISE IS IT?

to solve FOUNDATIONAL PROBLEMS we
ADAPT techniques from (mathematical) LOGIC

to SCRUTINISE
the VALIDITY of proposed FORMAL METHODS
we should CAUTIOUSLY ADAPT
METHODS from ANALYTIC PHILOSOPHY

REASONABLE SCEPTICISM

SYSTEMATIC DOUBT

PHILOSOPHICAL LOGIC
PHILOSOPHY OF MATHEMATICS
EPISTEMOLOGY
PHILOSOPHY OF SCIENCE

TYPES of JUSTIFICATION

JUSTIFICATION by ANALOGY

JUSTIFICATION by COST MEASUREMENTS

JUSTIFICATION by QUALITY MEASUREMENTS

JUSTIFICATION by COST ARGUMENTS

JUSTIFICATION by QUALITY ARGUMENTS

SCOPE of ARGUMENT

RANGE of METHODS

particular formal methods
certain kinds of formal method
all formal methods

EXTENT of APPLICATION

specifications
selective or partial proofs
full proofs

KINDS of APPLICATIONS

all applications
some applications
critical applications

JUSTIFIABILITY MATRIX

	specs	selective proof	full proof
all applications	X		
some applications	X	X	
critical applications	X	X	X

A Sample Argument

Testing of Software
(in most cases)
cannot be exhaustive

Given a formal specification
a correct program
can be proven correct

The justification of this claim
gets us immediately into
Philosophical deep water

EXPERIMENTAL SCIENCE	**MATHEMATICS & LOGIC**
A POSTERIORI CONTINGENT SYNTHETIC	**A PRIORI NECESSARY ANALYTIC**

SUBJECT TO DISPUTE

The DISTINCTION between
ANALYTIC and SYNTHETIC
(and the other categories)
(e.g. Quine)

The STATUS of MATHEMATICS
(e.g. Lakatos)

HOW to ESTABLISH
MATHEMATICAL TRUTHS
(and hence what they are)

HOW to APPLY
MATHEMATICAL TRUTHS