HOL88 and the future of HOL

Roger Bishop Jones

ICL Defence Systems

This document consists of the overheads for a presentation on HOL88 and the future of HOL, prepared for the ‘compusec’ meeting in APRIL 1989.

NEW FEATURES IN HOL88

FUTURE PROJECTS INVOLVING HOL

‘THE’ IED PROJECT

NEW FEATURES in HOL88 VERSION 1.05

LOOSE SPECIFICATIONS OF CONSTANTS
(as requested by ICL)

MULTIPLE CONSTANT INTRODUCTION

RECURSIVE TYPE DEFINITION PACKAGE
(developed by Tom Melham)

INTRODUCTION OF LIBRARIES

CUSTOMISABLE USER INTERFACE

IMPROVED ERROR MESSAGES

UNIX SYSTEM CALLS

FUTURE PROJECTS INVOLVING HOL

INTERFACING HOL to CATHEDRAL II
(ESPRIT BRA, CAMBRIDGE, PHILLIPS, IMEC)

TOTALLY VERIFIED SYSTEM
(software compiler and hardware)
(IED, INMOS, SRI, OXFORD, CAMBRIDGE)

INTERFACING HOL to ELLA
(IED PRAXIS BA CAMBRIDGE)

DOCUMENTATION for HOL
(AUSTRALIAN MOD, CAMBRIDGE, SRI)

FOUNDATIONS and TOOLS
for FORMAL VERIFICATION
(IED, ICL, PVL, CAMBRIDGE, KENT)

HOL IMPLEMENTATION in SML
at CALGARY

FOUNDATIONS and TOOLS for FORMAL VERIFICATION

PARTICIPANTS:

ICL Defence Systems

Program Validation Limited

University of Cambridge

University of Kent

OBJECTIVES:

High Quality, High Assurance re-implementation of HOL (in SML)

Improvements to usability and productivity

Extension to software verification

Link with SPADE tools

Development of Libraries

Foundational Studies

HIGH ASSURANCE IMPLEMENTATION of HOL

following LCF paradigm
SEPARATE OUT CRITICAL CODE
into abstract data type

FORMALLY SPECIFY
SYNTAX (in HOL) and SEMANTICS (in ZF-HOL)
of ABSTRACT HOL LOGIC

FORMALLY SPECIFY (in HOL)
ABSTRACT PROOF SYSTEM

INFORMALLY PROVE SOUNDNESS
of PROOF SYSTEM

IMPLEMENT CORE PROOF CHECKER
in HOL/ML

INFORMALLY PROOF CORRECTNESS
of IMPLEMENTATION

APPROACHES to CODE VERIFICATION using HOL

WRITE and VERIFY PROGRAMS
in INTERSECTION of HOL and ML

ADAPT SPADE TOOLS
to GENERATE
VERIFICATION CONDITIONS in HOL

define
PROGRAMMING LANGUAGE SEMANTICS
in HOL and
EMBED PROGRAM LOGICS
into HOL
(see MJCG paper)

TINKERING with the LOGIC

SCOPING of NAMES
(by using compound names)

OVERLOADING of NAMES
(disambiguation by type)

OVERLOADING of JUXTAPOSITION

MORE RADICAL CHANGES to LOGIC

FULL SUPPORT for MODULARITY
(with ML-like Polymorphism)

INTRODUCTION
of
DEPENDENT TYPES

RETREAT to PSEUDO-TYPES

REFLEXIVE FOUNDATIONS

CONVERGENCE with METALANGUAGE