What's Different About ICL HOL

Roger Bishop Jones
International Computers Limited, Eskdale Road,
Winnersh, Wokingham, Berks RG11 5TT

tel: 0734 693131 x6536, fax: 0734 697636
email: uucp: rbj@win0109.uucp

WHAT'S DIFFERENT ABOUT ICL-HOL

Objectives

What's the Same?

"System Level" Changes

Concrete Syntax

Theory Hierarchy

Goal Package

Proof Contexts

Rewriting

Resolution

Missing Bits

OBJECTIVES

INTEGRITY

ASSURANCE

SUPPORT FOR Z (& other notations)

PRODUCTIVITY

NOT intended to supplant Cambridge HOL

NOT oriented towards hardware verification

NOT compatible with Cambridge HOL

WHAT'S THE SAME

FOLLOWS "LCF PARADIGM"
(more closely than LCF and HOL?)

ABSTRACT LOGIC
(but not concrete syntax)

BASIC CONCEPTS

rules
conversions
tactics
...als
etc...

"SYSTEM LEVEL" DIFFERENCES

METALANGUAGE = Standard ML (with extensions)

THEORY DATABASE = PolyML database

hence

delete definition
delete theory

WATERTIGHT ABSTRACT DATA TYPE
(no "mk_thm")

CONCRETE SYNTAX

extended character set

well defined syntax and lexis for terms

user definable fixity and precedence

specification paragraphs

⌜if a then b else c⌝ instead of `"(a => b | c)"`

set abstraction simplified

ALIASES instead of INTERFACE MAPS

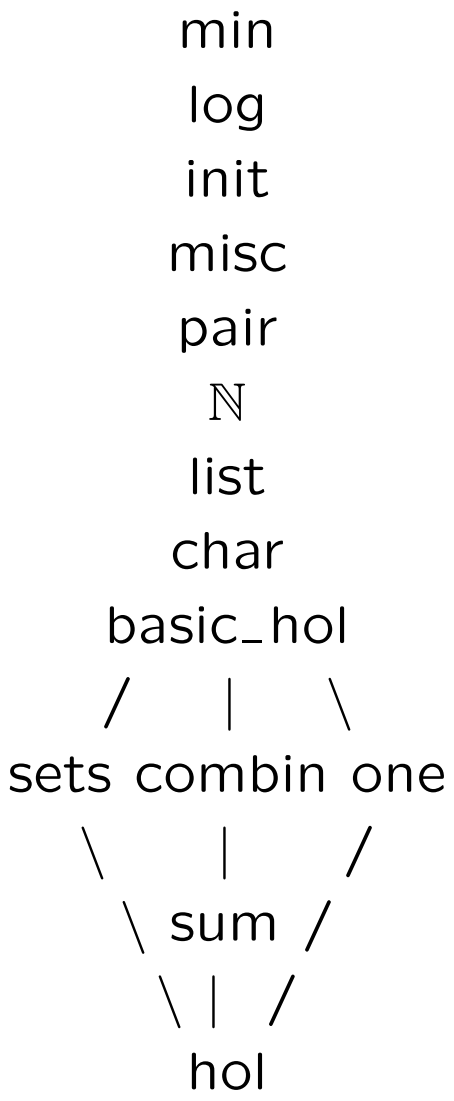
no “indeterminate types” error

“type-contexts” instead of “sticky types”

polymorphic type abbreviations

THEORY HIERARCHY

theories are "designed"



GOAL PACKAGE

Validation by Incremental Proof

Proves exactly the Goal

Proof Stack

Numbered Assumptions and Goals

Eliminates Duplicate Subgoals

Subgoals extra assumptions

Terms in Quotes (⌜t⌝)
Numbers in Comments ((* 4 *))

PROOF CONTEXTS

PROOF CONTEXTS CONTROL:

- Basic rewrites
- Stripping of concls and asms
- Rewrite canonicalisation
- Auto Proof
- Consistency Proof

STRIPPING

effects extended through proof context

e.g. solves propositional tautologies

REWRITING

fails if no rewriting

does not instantiate free variables in theorems used for rewriting

“basic rewrites” taken from proof context (and usually include conversions as well as theorems)

RESOLUTION

no equivalent to Cambridge-HOL resolution

manual instantiation of assumptions
sometimes does the job

first-order resolution package using
unification supported

MISSING BITS

words, concrete data types

term surgery, libraries

restricted quantification

user programmable type-checking for HOL