Guide to HOL4 interaction and basic proofs

Magnus O. Myreen

1 Introduction

This document gives readers, with no experience in using HOL4, the most minimum knowledge needed to start using HOL4. The aim is to give a concise description of the basics in a format usable as a beginners' reference manual.

Section 2: Interaction with HOL4 (via emacs or xemacs)
Section 3: Searching for theorems and theories
Section 4: Common proof tactics
Section 5: Further reading and general advice

The text assumes that the reader has HOL4 installed from: `http://hol.sf.net/`.

2 Interaction with HOL4 (via emacs or xemacs)

Michael Norrish has written an emacs script which makes interaction with HOL easy. To install the script add this line to your `.emacs` file:

```
(load "<path>/HOL/tools/hol-mode")
```

Replace `<path>` with the full path to your HOL4 installation. To make emacs highlight the active region, also add the following line to your `.emacs` file:

```
(transient-mark-mode 1)
```

Restart emacs to make these changes take effect.

2.1 Starting a HOL4 session

1. Start emacs.
2. Press `C-x C-f` to open a file for your proof script.
3. Press `C-x 3` to split the emacs window into two columns.
4. Press `M-h h` to start HOL4.
5. Press `C-x o` to move cursor to the other window (where we type).

The HOL window should look something like this:

```
------------------------------------------------------------------
       HOL-4 [Kananaskis 5 (built Thu Feb 21 08:37:11 2008)]

       For introductory HOL help, type: help "hol";
------------------------------------------------------------------

[loading theories and proof tools ..... ]
[closing file "/local/scratch/user/HOL/tools/end-init-boss.sml"]
-
```

2.2 Copying input into HOL4 (Opening a theory)

1. Select text by pressing `C-space` at one end of the text.
2. Copy the region into HOL4 by pressing `M-h M-r` at the other end. (You can also use drag the mouse to select text to be sent to HOL.)

For example, pressing `C-space` then `M-h M-r` around the following line

```
open arithmeticTheory listTheory;
```

makes HOL4 open the library theories for arithmetic (over natural numbers) and lists. HOL4 prints a long list of definitions and already proved results.

2.3 Starting a goal-oriented proof

Most HOL4 proofs are constructed using an interactive *goal stack* and then put together using the ML function `prove` (Section 2.6, 2.7). To start the goal stack:

1. Write a goal, *e.g.* `‘!n. n < n + 1‘`, (we write ∀ as `!` in HOL4).
2. Move the cursor inside the back-quotes (‘).
3. Press `M-h g` to push the goal onto the goal stack.

The HOL4 window should look something like this:

```
- > val it =
    Proof manager status: 1 proof.
    1. Incomplete:
         Initial goal:
         !n. n < n + 1

     : proofs
- > val it = () : unit
```

2.4 Applying a tactic

Make progress in a proof using *proof tactics*.

1. Write the name of a tactic, *e.g.* `DECIDE_TAC`, see Section 4 for more tactics
2. Press `C-space` at one end of the text.
3. Move the cursor to the other end of the text.
4. Press `M-h e` to apply the tactic.

A tactic makes HOL4 update the current goal. The HOL4 window will either display the new goal(s) or print:

```
Initial goal proved.
|- !n. n < n + 1 : goalstack
```

You can undo the effect of the applied tactic by pressing `M-h b`. Press `M-h p` to view the current goal.

`M-h h`	– start HOL	`M-h g`	– push goal onto goal stack
`M-h M-r`	– copy region into HOL	`M-h e`	– apply tactic to goal
`M-h C-t`	– display types on/off	`M-h b`	– move back in proof
`M-h C-c`	– interrupt HOL	`M-h p`	– print current goal
		`M-h d`	– drop current goal

Figure 1: Most important key bindings in the emacs HOL4 mode.

2.5 Ending a goal-oriented proof

One can pop goals off the goal stack by pressing `M-h d`, which gives:

```
- - OK..
> val it = There are currently no proofs. : proofs
```

2.6 Saving the resulting theorem

One can use `prove` to store the result of a proof (called a *theorem*), *e.g.* the following stores the theorem $\forall n.\ n < n + 1$ in an ML variable `LESS_ADD_1`:

```
val LESS_ADD_1 = prove(`` !n. n < n + 1 ``,DECIDE_TAC);
```

When the above line is copied into HOL4 (using `C-space` then `M-h M-r`, as described in Section 2.2), HOL4 responds with:

```
- > val LESS_ADD_1 = |- !n. n < n + 1 : thm
```

2.7 Saving proofs based on multiple tactics

Suppose we have proved the goal `` `!n. n <= n * n` `` with the following tactics:

```
Induct_on `n`                   (* comment: induction on n  *)

  DECIDE_TAC                    (* comment: solve base case *)

  ASM_SIMP_TAC bool_ss [MULT]   (* comment: simplify goal   *)
  DECIDE_TAC                    (* comment: solve step case *)
```

Tactics can be pieced together for `prove` using `THEN` and `THENL`:

```
val LESS_EQ_MULT = prove(`` !n. n <= n * n ``,
  Induct_on `n` THENL [
    DECIDE_TAC,
    ASM_SIMP_TAC bool_ss [MULT] THEN
    DECIDE_TAC]);
```

Copy the above into HOL4 using `C-space` then `M-h M-r`, as in Section 2.2.

2.8 Displaying types in HOL4

HOL4 does not by default display types. Press `M-h C-t` to switch printing of type information on or off.

2.9 Interrupting HOL4

Press `M-h C-c` to interrupt HOL4 — useful when a tactic fails to terminate (*e.g.* `METIS_TAC` often fails to terminate when unsuccessfully applied).

2.10 Making a definition

Function can be defined using `Define`, *e.g.* square is defined as follows.

```
val SQUARE_def = Define `SQUARE n = n * n`;
```

Data-types are defined using `Hol_datatype`, *e.g.* a binary tree which holds values of type `'a` (a type variable) at the leaves:

```
val _ = Hol_datatype `TREE = LEAF of 'a | BRANCH of TREE => TREE`;
```

A valid tree is *e.g.* `BRANCH (LEAF 5) (BRANCH (LEAF 1) (LEAF 7))` with type `num TREE`, where `num` is the type name for a natural number. We can define recursive functions, *e.g.*

```
val MAP_TREE_def = Define `
  (MAP_TREE f (LEAF n) = LEAF (f n)) /\
  (MAP_TREE f (BRANCH u v) = BRANCH (MAP_TREE f u) (MAP_TREE f v))`;
```

`SQUARE_def` and `MAP_TREE_def` are theorems containing the above definitions. Theorems describing `TREE` can be retrieved by coping the following into HOL4 (by pressing `C-space` then `M-h M-r`, Section 2.2).

```
val TREE_11 = fetch "-" "TREE_11";
val TREE_distinct = fetch "-" "TREE_distinct";
```

2.11 Making a theory

Proofs and definitions are stored in files called scripts, *e.g.* we can store the definitions from above in a file called `mytreeScript.sml`, which should begin with the lines

```
open HolKernel boolLib bossLib Parse;
val _ = new_theory "mytree";
```

and end with the line

```
val _ = export_theory();
```

Replace `prove` by `store_thm` for results you wish to export from the theory, *e.g.*

```
val LESS_ADD_1 = store_thm("LESS_ADD_1",``!n.n<n+1``,DECIDE_TAC);
```

Make sure your script only consists of ML definitions (`val x = y`, `fun g x = y`), open commands (`open x y z`) and comments `(* comment *)`.

The theory `mytreeTheory` is created by executing `Holmake` in the directory where `mytreeScript.sml` is stored. A readable version of the theory is stored under `mytreeTheory.sig`.

3 Searching for theorems and theories

HOL4 has a large collection of library theories. The most commonly used are:

`arithmeticTheory`	– natural numbers, *e.g.* `0, 1, 2, SUC 0, SUC 6`
`listTheory`	– lists, *e.g.* `[1;2;3] = 1::2::3::[], HD xs`
`pred_setTheory`	– simple sets *e.g.* `{1;2;3}, x IN s UNION t`
`pairTheory`	– pairs/tuples *e.g.* `(1,x), (2,3,4,5), HD (x,y)`
`wordsTheory`	– n-bit words *e.g.* `0w:word32, 1w:'a word, x !! 1w`

Other standard theories include:

```
arithmeticTheory  bagTheory  boolTheory  combinTheory  fcpTheory
finite_mapTheory  fixedPointTheory  floatTheory  integerTheory
limTheory  optionTheory  probTheory  ratTheory  realTheory
relationTheory  rich_listTheory  ringTheory  seqTheory
sortingTheory  state_transformerTheory  stringTheory  sumTheory
topologyTheory  transcTheory  whileTheory
```

The library theories are conveniently browsed using the following HTML reference page (created when HOL4 is compiled). Replace `<path>` with the path to your HOL4 installation.

```
<path>/HOL/help/HOLindex.html
```

Once theories has been opened (see Section 2.2), one can search for theorems in the current context using `DB.match`, *e.g.* with `arithmeticTheory` opened,

```
DB.match [] ``n DIV m <= k``
```

prints a list of theorems containing n `DIV` $m \leq k$ for some n, m, k:

```
[(("arithmetic", "DIV_LE_MONOTONE"),
  (|- !n x y. 0 < n /\ x <= y ==> x DIV n <= y DIV n, Thm)),
 (("arithmetic", "DIV_LE_X"),
  (|- !x y z. 0 < z ==> (y DIV z <= x = y < (x + 1) * z), Thm)),
 (("arithmetic", "DIV_LESS_EQ"),
  (|- !n. 0 < n ==> !k. k DIV n <= k, Thm))]
```

Try to write increasingly specific queries if the returned list is long, *e.g.* `DB.match [] ``n DIV m``` returns a list of length 32. Note that `DB.match [] ``DIV``` does not work since `DIV` is an infix operator, but `DB.match [] ``$DIV``` works.

4 Common proof tactics

Most HOL4 proofs are carried out by stating a goal and then applying *proof tactics* that reduce the goal. This section describes basic use of the most important proof tactics. Press `C-space` then `M-h e` to apply a tactic (Section 2.4).

4.1 Automatic provers

Simple goals can often be proved automatically by `METIS_TAC`, `DECIDE_TAC` or `EVAL_TAC`. `METIS_TAC` is first-order prover which is good at general problems, but requires the user to supply a list of relevant theorems, *e.g.* the following goal is proved by `METIS_TAC [MOD_TIMES2,MOD_MOD,MOD_PLUS]`.

```
!k. 0 < k ==> !m p n. (m MOD k * p + n) MOD k = (m * p + n) MOD k
```

DECIDE_TAC handles linear arithmetic over natural numbers, *e.g.* DECIDE_TAC solves:

```
!m n k. m < n /\ n < m+k /\ k <= 3 /\ ~(n = m+1) ==> (n = m+2)
```

EVAL_TAC is good at fully instantiated goals, *e.g.* EVAL_TAC solves:

```
0 < 5 /\ (HD [4;5;6;7] + 2**32 = 3500 DIV 7 + 4294966800)
```

4.2 Proof set-up

Goals that contain top-level universal quantifiers (!x.), implication (==>) or conjunction (/\) are often taken apart using REPEAT STRIP_TAC or just STRIP_TAC, *e.g.* the goal ‘!x. (!z. x < h z) ==> ?y. f x = y‘ becomes the following. (Assumptions are written under the line.)

```
?y. f x = y
------------------------------------
  !z. x < h z
```

4.3 Existential quantifiers

Goals that have a top-level existential quantifier can be given a witness using Q.EXISTS_TAC, *e.g.* Q.EXISTS_TAC ‘1‘ applied to goal ?n. !k. n * k = k produces goal !k. 1 * k = k.

4.4 Rewrites

Most HOL4 proofs are based on rewriting using equality theorems, *e.g.*

```
ADD_0:            |- !n. n + 0 = n
LESS_MOD:         |- !n k. k < n ==> (k MOD n = k)
```

ASM_SIMP_TAC and FULL_SIMP_TAC are two commonly used rewriting tactics, *e.g.* suppose the goal is the following:

```
5 + 0 + m = (m MOD 10) + (5 MOD 8)
------------------------------------
  0.  p = 2 + 0 + (m MOD 10)
  1.  m < 10
```

ASM_SIMP_TAC bool_ss [ADD_0,LESS_MOD] rewrites the goal using the supplied theorems together with the current goal's assumptions and some boolean simplifications bool_ss:

```
5 + m = m + (5 MOD 8)
------------------------------------
  0.  p = 2 + 0 + (m MOD 10)
  1.  m < 10
```

FULL_SIMP_TAC bool_ss [ADD_0,LESS_MOD] does the same except that it also applies the rewrites to the assumptions:

```
5 + m = m + (5 MOD 8)
------------------------------------
  0.  p = 2 + m
  1.  m < 10
```

`bool_ss` can be replaced by `std_ss`, which is a stronger simplification set that would infer `5 < 8` and hence simplify `5 MOD 8` as well. I recommend that the interested reader also reads about `AC`, `Once` and `SRW_TAC`.

4.5 Induction

Use the tactic `Induct_on ‘x‘` to start an induction on `x`. Here `x` can be any variable with a recursively defined type, *e.g.* a natural number, a list or a `TREE` as defined in Section 2.10. One can start a complete (or strong) induction over the natural number `n` using `completeInduct_on ‘n‘`.

4.6 Case splits

A goal can be split into cases using `Cases_on ‘x‘`. The goal is split according to the constructors of the type of `x`, *e.g.* for the following goal

```
!x. ~(x = []) ==> (x = HD x::TL x)
```

`Cases_on ‘x‘` splits the goal into two:

```
~(h::t = []) ==> (h::t = HD (h::t)::TL (h::t))

~([] = []) ==> ([] = HD []::TL [])
```

Case splits on boolean expressions are also useful, *e.g.* `Cases_on ‘n < 5‘`.

4.7 Subproofs

It is often useful to start a mini-proof inside a larger proof, *e.g.* for the goal

```
foo n
------------------------------------
  0 < n
```

we might want to prove `h n = g n` assuming `0 < n`. We can start such a subproof by typing `‘h n = g n‘ by ALL_TAC`.[1] The new goal stack:

```
foo n
------------------------------------
  0.  0 < n
  1.  h n = g n

h n = g n
------------------------------------
  0 < n
```

If `‘h n = g n‘` can be proved in one step, *e.g.* using `METIS_TAC [MY_LEMMA]`, then apply `‘h n = g n‘ by METIS_TAC [MY_LEMMA]` instead of `‘h n = g n‘ by ALL_TAC`. If the sub-goal requires multiple steps the tactic after the `by` will need to be parenthesised: `‘`*goal*`‘ by (`*tac*$_1$ `THEN` *tac*$_2$ `...)`

[1] You can also use the emacs binding `M-h M-s` with the cursor inside the sub-goal.

4.8 Proof by contradiction

Use `CCONTR_TAC` to add the negation of the goal to the assumptions. The task is then to prove that one of the assumptions of the goal is false. One can *e.g.* add more assumptions using `` `...` by ALL_TAC ``, described above, until one assumption is the negation of another assumption (and then apply `METIS_TAC []`).

4.9 More tactics

An HTML reference of all tactics and proof tools is created when HOL4 is compiled. Replace `<path>` with the path to your HOL4 installation.

```
<path>/HOL4/help/src/htmlsigs/idIndex.html
```

The reference provides an easy way to access both the implementations of tactics as well as their documentation (where such exists). The interested reader may want to look up the following:

```
CONV_TAC  DISJ1_TAC  DISJ2_TAC  MATCH_MP_TAC  MP_TAC  PAT_ASSUM  Q
```

5 Further reading and general advice

General advice on using HOL4:

1. State definitions carefully with the subsequent proofs in mind.
2. Make proofs reusable by splitting them into multiple small lemmas.
3. Strive to make the most of library theories and rewriting.

One can only learn HOL4 via examples, so try proving something. Example problems and solutions are presented in the *HOL Tutorial*, available under:

```
http://hol.sf.net/documentation.html
```

The same page also contains:

HOL Description – a description of the HOL4 system
HOL Reference – a detailed descriptions of proof tactics and other tools
HOL Logic – a presentation of the underlying logic

For day-to-day look-ups, I find `DB.match` (illustrated in Section 3) and the HTML reference (mentioned in Section 4.9) most helpful.