The growing logical system of hol_light and nhol

August 20, 2013

Contents

Chapter 1

Introduction

This is an attempt to describe the growing logical system of hol_light and Nhol through the modules in the order they are evaluated. Rules, theorems and proofs are introduced in a graphical way as consisely as possible to be easier to memorize.

Errors could be find because I write this document as my notes while I'm learning the system. Most of all, the document is absolutely not complete even in the chapters already written.

Some notes are based on the hol_light official documentation, while proofs, where present, are rebuilt through an analysis of the code.

I've used the fitch syle for the proofs, probably in an odd way: mixing the sequent format on which hol_light is based with the fitch style. The sequent format carries the assumptions with the conclusion so there should be no reason to indent for showing that a statement is derived from a prevous assumption, because this is already visible in the same line of the statement. Anyway I wanted to mantain the indentation to give a graphical hint of the flow of the proof.

Chapter 2

The language

Module	Types		Constants			Infixes		
	Name	Arity	Name	Type	Notes	Constant Name	Precedence	Infix hand
fusion	bool	0						
fusion	fun	2						
fusion			=	$\alpha \to \alpha \to bool$				
bool						=	12	right
bool			<=>	$bool \to bool \to bool$	$(=) : \ bool \to bool \to bool$		2	right
bool			T	$bool$				

Part I

Module Fusion

Chapter 3

Primitive Inference Rules

3.1 REFL

val REFL : term $\rightarrow$ thm

$$\frac{}{\vdash s = s} \text{ REFL}$$

$s : \alpha$

3.2 TRANS

val TRANS : thm $\rightarrow$ thm $\rightarrow$ thm

$$\frac{\Gamma \vdash s = t \quad \Delta \vdash t = u}{\Gamma \cup \Delta \vdash s = u} \text{ TRANS}$$

$s, t, u : \alpha$

3.3 MK_COMB

val MK_COMB : (thm * thm) $\rightarrow$ thm

$$\frac{\Gamma \vdash s = t \quad \Delta \vdash u = v}{\Gamma \cup \Delta \vdash s(u) = t(v)} \text{ MK\_COMB}$$

$s, t : \alpha \rightarrow \beta$ and $u, v : \alpha$

3.4 ABS

val ABS : term $\rightarrow$ thm $\rightarrow$ thm

$$\frac{\Gamma \vdash s = t}{\Gamma \vdash (\lambda x.\ s) = (\lambda x.\ t)} \text{ ABS}$$

$s, t : \alpha$ and $x : \beta$

3.5 BETA

val BETA : term → thm

$$\frac{}{\vdash (\lambda x.\, t)\ x = t}\ \text{BETA}$$

$t : \alpha$ and $x : \beta$

3.6 ASSUME

val ASSUME : term → thm

$$\frac{}{\{p\} \vdash p}\ \text{ASSUME}$$

$p : \mathit{bool}$

3.7 EQ_MP

val EQ_MP : thm → thm → thm

$$\frac{\Gamma \vdash p = q \quad \Delta \vdash p}{\Gamma \cup \Delta \vdash p}\ \text{EQ\_MP}$$

$p, q : \mathit{bool}$

3.8 DEDUCT_ANTISYM_RULE

val DEDUCT_ANTISYM_RULE : thm → thm → thm

$$\frac{\Gamma \vdash p \quad \Delta \vdash q}{(\Gamma - \{q\}) \cup (\Delta - \{p\}) \vdash p = q}\ \text{DEDUCT\_ANTISYM\_RULE}$$

$p, q : \mathit{bool}$

3.9 INST

val INST : (term * term) list → thm → thm

$$\frac{\Gamma[x_1, \ldots, x_n] \vdash p[x_1, \ldots, x_n]}{\Gamma[t_1, \ldots, t_n] \vdash p[t_1, \ldots, t_n]}\ \text{INST}$$

$p : \mathit{bool}$ and $t_i, x_i : \alpha$

3.10 INST_TYPE

val INST_TYPE : (hol_type * hol_type) list → thm → thm

$$\frac{\Gamma[\alpha_1,\ldots,\alpha_n] \vdash p[\alpha_1,\ldots,\alpha_n]}{\Gamma[\gamma_1,\ldots,\gamma_n] \vdash p[\gamma_1,\ldots,\gamma_n]}\ \mathrm{INST\_TYPE}$$

$p : \mathit{bool}$

Part II

Module Equal

Chapter 4

BETA_CONV

General case of beta conversion: BETA is the special case where the argument is the same as the bound variable

val BETA_CONV : term → thm

$$\frac{}{\vdash (\lambda x.\ u)\ v = u[v/x]}\ \mathrm{BETA\_CONV}$$

$v : \sigma$, $u : \tau$ and $x : \upsilon$

Chapter 5

Derived equality rules

5.1 AP_TERM

Applies a function to both sides of an equational term.

val AP_TERM : term → thm → thm

$$\frac{\Gamma \vdash x = y}{\Gamma \vdash f\ x = f\ y}\ \text{AP\_TERM}$$

$f : \sigma \to \tau$ and $x, y : \sigma$

1	$\Gamma \vdash x = y$	given	
2	$\vdash f = f$	REFL	
3	$\Gamma \vdash f\ x = f\ y$	MK_COMB, 1,2	

5.2 AP_THM

Proves equality of equal functions applied to a term

val AP_THM : thm → term → thm

$$\frac{\Gamma \vdash f = g}{\Gamma \vdash f\ x = g\ x}\ \text{AP\_THM}$$

$f, g : \sigma \to \tau$ and $x : \sigma$

1	$\Gamma \vdash f = g$	given	
2	$\vdash x = x$	REFL	
3	$\Gamma \vdash f\ x = g\ x$	MK_COMB, 1,2	

5.3 SYM

Swaps left-hand and right-hand sides of an equation.

val SYM : thm → thm

$$\frac{\Gamma \vdash t_1 = t_2}{\Gamma \vdash t_2 = t_1} \text{ SYM}$$

$t_1, t_2 : \sigma$

1	$\Gamma \vdash t_1 = t_2$	given
2	$\vdash t_1 = t_1$	REFL
3	$\Gamma \vdash (=)\, t_1 = (=)\, t_2$	AP_TERM, 1
4	$\Gamma \vdash t_1 = t_1 \mathrel{<=>} t_2 = t_1$	MK_COMB, 3,2
5	$\Gamma \vdash t_2 = t_1$	EQ_MP, 4,2

5.4 ALPHA

Proves equality of alpha-equivalent terms.

val ALPHA : term → term → thm

$$\frac{}{\vdash t_1 = t_2} \text{ ALPHA}$$

where $t_1, t_2 : \sigma$ are alpha-equivalent term
(i.e. they are different only for the name of their bound variables)

1	$\vdash t_1 = t_1$	REFL
2	$\vdash t_2 = t_2$	REFL
3	$\vdash t_1 = t_2$	TRANS, 1,2

Note that `TRANS` succeeds because t_1 and t_2 are alpha-equivalent.

Chapter 6

Conversions

6.1 ALPHA_CONV

val ALPHA_CONV : term $\to$ term $\to$ thm

$$\frac{}{\vdash (\lambda x.\ t) = (\lambda y.\ t[y/x])}\ \mathrm{ALPHA\_CONV}$$

where $x, y : \alpha$ and y does not occur free in t.

1	$\vdash (\lambda x.\ t) = (\lambda y.\ t[y/x])$	ALPHA_CONV
2	$\vdash b\ (\lambda x.\ t) = b\ (\lambda y.\ t[y/x])$	AP_TERM b

6.2 GEN_ALPHA_CONV

Provides alpha conversion for lambda abstraction of the form $\lambda x.\ t$ as well as for terms of the form $b\ (\lambda x.\ t)$ such as quantifiers and other binders.

val GEN_ALPHA_CONV : term $\to$ term $\to$ thm

$$\frac{}{\vdash (\lambda x.\ t) = (\lambda y.\ t[y/x])}\ \mathrm{GEN\_ALPHA\_CONV}$$

1	$\vdash (\lambda x.\ t) = (\lambda y.\ t[y/x])$	ALPHA_CONV

$$\frac{}{\vdash b\ (\lambda x.\ t) = b\ (\lambda y.\ t[y/x])}\ \mathrm{GEN\_ALPHA\_CONV}$$

1	$\vdash (\lambda x.\ t) = (\lambda y.\ t[y/x])$	ALPHA_CONV
2	$\vdash b\ (\lambda x.\ t) = b\ (\lambda y.\ t[y/x])$	AP_TERM b

Part III

Module Bool

Chapter 7

Usefull derived rules

7.0.1 PROVE_HYP: the Cut Rule

Eliminates a provable assumption from a theorem.

Note that for this rule to be usefull the conclusion of the first theorem should be the same as an assumption of the second theorem.

val PROVE_HYP : thm → thm → thm

$$\frac{\Gamma \vdash p \quad \Delta, p \vdash q}{\Gamma \cup \Delta \vdash q}\ \text{PROVE\_HYP}$$

If the conclusion of first theorem is not in the assumption of the second.

$$\frac{\Gamma \vdash p \quad \Delta \vdash q}{\Delta \vdash q}\ \text{PROVE\_HYP}$$

Proof of the significant case (the other is trivial since the derived is one of the given theorems):

1	$\Gamma \vdash p$	given
2	$\Delta, p \vdash q$	given
3	$\Delta \cup \Gamma \vdash p \Leftrightarrow q$	DEDUCT_ANTISYM_RULE, 1,2
4	$\Delta \cup \Gamma \vdash q$	EQ_MP, 3,1

Chapter 8

Derived rules for classical connectives

Classical connectives are introduced as definitions

8.1 Rules on Truth

8.1.1 T_DEF

$\vdash \top \Leftrightarrow (\lambda p.\ p) = (\lambda p.\ p)$

$p : bool$

8.1.2 TRUTH

val TRUTH : thm

$$\frac{}{\vdash \top}\ \mathrm{TRUTH}$$

1	$\vdash \top \Leftrightarrow (\lambda p.\ p) = (\lambda p.\ p)$	T_DEF
2	$\vdash \lambda p.\ p = \lambda p.\ p$	REFL
3	$\vdash (\lambda p.\ p) = (\lambda p.\ p) \Leftrightarrow \top$	SYM, 1
4	$\vdash \top$	EQ_MP, 3,2

8.1.3 EQT_ELIM

val EQT_ELIM : thm $\rightarrow$ thm

$$\frac{\Gamma \vdash p \Leftrightarrow \top}{\Gamma \vdash p}\ \mathrm{EQT\_ELIM}$$

$p : bool$

1	$\Gamma \vdash p \Leftrightarrow \top$	given
2	$\vdash \top$	TRUTH
3	$\Gamma \vdash \top \Leftrightarrow p$	SYM, 1
4	$\Gamma \vdash p$	EQ_MP, 3,2

8.1.4 EQT_INTRO

val EQT_INTRO : thm $\rightarrow$ thm

$$\frac{\Gamma \vdash p}{\Gamma \vdash p \Leftrightarrow \top}\ \text{EQT\_INTRO}$$

$p : bool$

1	$\Gamma \vdash p$	given
2	$t \vdash t$	ASSUME
3	$\vdash \top$	TRUTH
4	$t \vdash t \Leftrightarrow \top$	DEDUCT_ANTISYM_RULE, 2,3
5	$t \Leftrightarrow \top \vdash t \Leftrightarrow \top$	ASSUME
6	$t \Leftrightarrow \top \vdash t$	EQT_ELIM, 5
7	$\vdash t \Leftrightarrow t \Leftrightarrow \top$	DEDUCT_ANTISYM_RULE, 6,4
8	$\vdash p \Leftrightarrow p \Leftrightarrow \top$	INST $[p/t]$, 7
9	$\Gamma \vdash p \Leftrightarrow \top$	EQ_MP, 8,1

8.2 Rules on And

8.2.1 AND_DEF

$$\vdash \wedge \Leftrightarrow \lambda p\, \lambda q.\ (\lambda f.\ f\ p\ q) = (\lambda f.\ f\ \top\ \top)$$

$f : bool \rightarrow bool \rightarrow bool$ and $p, q : bool$

8.2.2 CONJ

val CONJ : thm $\rightarrow$ thm $\rightarrow$ thm

$$\frac{\Gamma \vdash th1, \Delta \vdash th2}{\Gamma \cup \Delta \vdash th1 \wedge th2}\ \text{CONJ}$$

$p : bool$

1	$\Gamma \vdash th1$	given
2	$\Delta \vdash th2$	given
3	$p \vdash p$	ASSUME
4	$p \vdash p \Leftrightarrow \top$	EQT_INTRO, 3
5	$p \vdash f\ p = f\ \top$	AP_TERM f, 4
6	$q \vdash q$	ASSUME
7	$q \vdash q \Leftrightarrow \top$	EQT_INTRO, 6
8	$p, q \vdash f\ p\ q \Leftrightarrow f\ \top\ \top$	MK_COMB, 5,7
9	$p, q \vdash (\lambda f.\ f\ p\ q) = (\lambda f.\ f\ \top\top)$	ABS f, 8
10	$\vdash (\wedge) = (\lambda p\ \lambda q.\ (\lambda f.\ f\ p\ q) = (\lambda f.\ f\ \top\ \top))$	AND_DEF
11	$\vdash (\wedge)\ p = (\lambda p\ \lambda q.\ (\lambda f.\ f\ p\ q) = (\lambda f.\ f\ \top\ \top))\ p$	AP_THM p, 10
12	$\vdash p \wedge q \Leftrightarrow (\lambda p\ \lambda q.\ (\lambda f.\ f\ p\ q) = (\lambda f.\ f\ \top\top))\ p\ q$	AP_THM q, 11
13	$\vdash p \wedge q \Leftrightarrow (\lambda f.\ f\ p\ q) = (\lambda f.\ f\ T\ T)$	BETA_RULE, 12
14	$\vdash (\lambda f.\ f\ p\ q) = (\lambda f.\ f\ \top\ \top) \Leftrightarrow p \wedge q$	SYM, 13
15	$p, q \vdash p \wedge q$	EQ_MP, 14,9
16	$th1, th2 \vdash th1 \wedge th2$	INST, 15
17	$\Gamma \cup \{th2\} \vdash th1 \wedge th2$	PROVE_HYP, 1,16
18	$\Gamma \cup \Delta \vdash th1 \wedge th2$	PROVE_HYP, 2,17

Part IV

Module Simp

Chapter 9

mk_rewrites

9.1 IMP_CONJ_CONV

1	$p \Rightarrow q \Rightarrow r \vdash p \Rightarrow q \Rightarrow r$	ASSUME
2	$p \wedge q \vdash p \wedge q$	ASSUME
3	$p \wedge q \vdash p$	CONJUCNT1, 2
4	$p \wedge q, p \Rightarrow q \Rightarrow r \vdash q \Rightarrow r$	MP, 1,3
5	$p \wedge q \vdash q$	CONJUCNT2, 2
6	$p \wedge q, p \Rightarrow q \Rightarrow r \vdash r$	MP, 4,5
7	$p \Rightarrow q \Rightarrow r \vdash p \wedge q \Rightarrow r$	DISCH $(p \wedge q)$,6
8	$\vdash (p \Rightarrow q \Rightarrow r) \Rightarrow (p \wedge q \Rightarrow r)$	DISCH $(p \Rightarrow q \Rightarrow r)$,7
9	$p \wedge q \Rightarrow r \vdash p \wedge q \Rightarrow r$	ASSUME
10	$p \vdash p$	ASSUME
11	$q \vdash q$	ASSUME
12	$p, q \vdash p \wedge q$	CONJ, 10,11
13	$p, q, p \wedge q \Rightarrow r \vdash r$	MP, 9,12
14	$p, p \wedge q \Rightarrow r \vdash q \Rightarrow r$	DISCH q, 13
15	$p \wedge q \Rightarrow r \vdash p \Rightarrow q \Rightarrow r$	DISCH p, 14
16	$\vdash (p \wedge q \Rightarrow r) \Rightarrow (p \Rightarrow q \Rightarrow r)$	DISCH $p \wedge q \Rightarrow r$, 15
17	$\vdash p \Rightarrow (q \Rightarrow r) \Leftrightarrow p \wedge q \Rightarrow r$	IMP_ANTISYM_RULE, 8, 16

Chapter 10

Theorems Proofs

10.1 EQ_REFL

1	$x : \alpha = x$	REFL
2	$\forall x : \alpha.\, x = x$	GEN, 1