Implicational rewriting
User manual

Vincent Aravantinos

Hardware Verification Group
Concordia University

1 Introduction.

This document is the user manual of the "impconv" HOL Light library. It provides essentially two tactics `IMP_REWRITE_TAC` and `TARGET_REWRITE_TAC`.

Status of this document: This manual is a draft. It does not claim exhaustiveness nor perfect mathematical presentation of the specifications. However it should be sufficient for a quick start with implicational rewriting. It also does not cover all the functions that are available in the library, in particular those related to implicational conversions. Next versions of this documentation as well as an upcoming paper will provide more information.

Installation. To make use of the tactics and functions provided by this library, just type in the following inside a HOL Light session:

```
> needs "target_rewrite.ml";;
```

2 Implicational rewrite.

Informal specification: given a theorem of the form $\forall x_1 \cdots x_n.\ P \Rightarrow \forall y_1 \cdots y_m.\ l = r$, replace any occurrence of l by r in the goal, even if P does not hold. This may involve adding adding some propositional atoms (typically instantations of P) or existentials, but in the end, you are (almost) sure that l is replaced by r.

Tactic:

`IMP_REWRITE_TAC` : `thm list` $\rightarrow$ `tactic`

Given a list of theorems $[\mathtt{th}_1; \cdots; \mathtt{th}_k]$ of the form $\forall \mathtt{x}_1 \cdots \mathtt{x}_n.\ \mathtt{P} \Rightarrow \forall \mathtt{y}_1 \cdots \mathtt{y}_m.\ \mathtt{l} = \mathtt{r}$, `IMP_REWRITE_TAC` $[\mathtt{th}_1; \cdots; \mathtt{th}_k]$ applies as many implicational rewrites as it can with $\mathtt{th}_1$. When no more implicational rewrites can be achieved, do the same with $\mathtt{th}_2$, etc. When $\mathtt{th}_k$ is reached, start over from $\mathtt{th}_1$. Repeat till no more rewrite can be achieved.

Preprocessing:

- A theorem of the form $\forall x_1 \cdots x_n.\ P \Rightarrow \forall y_1 \cdots y_m.\ Q$ is turned into $\forall x_1 \cdots x_n.\ P \Rightarrow \forall y_1 \cdots y_m.\ Q = true$
  (try it: allows to use `IMP_REWRITE_TAC` *as a* deep `MATCH_MP_TAC`*);*
- A theorem of the form $\forall x_1 \cdots x_n.\ P \Rightarrow \forall y_1 \cdots y_m.\ \neg Q$ is turned into $\forall x_1 \cdots x_n.\ P \Rightarrow \forall y_1 \cdots y_m.\ Q = false$;
- A theorem of the form $\forall x_1 \cdots x_n.\ l = r$ is turned into $\forall x_1 \cdots x_n.\ true \Rightarrow l = r$
  (try it: allows to use `IMP_REWRITE_TAC` *as a substitute for* `REWRITE_TAC` *or even* `SIMP_TAC`*);*
- If the theorem has free variables then those are added to the universally quantified $x_1, \cdots, x_n$;
- A theorem of the form $\forall x_1 \cdots x_n.\ P \Rightarrow \forall y_1 \cdots y_k.\ Q \cdots \Rightarrow l = r$ is turned into $\forall x_1 \cdots x_n, y_1 \cdots y_k, \cdots P \wedge Q \wedge \cdots \Rightarrow l = r$;
- A theorem of the form $\forall x_1 \cdots x_n.\ P \Rightarrow (\forall y_1^1 \cdots y_k^1.\ Q_1 \cdots \Rightarrow l_1 = r_1 \wedge \forall y_1^2 \cdots y_k^2.\ Q_2 \cdots \Rightarrow l_2 = r_2 \wedge \cdots)$ is turned into the list of theorems $\forall x_1 \cdots x_n, y_1^1 \cdots y_k^1, \cdots P \wedge Q_1 \wedge \cdots \Rightarrow l_1 = r_1$, $\forall x_1 \cdots x_n, y_1^2 \cdots y_k^2, \cdots P \wedge Q_2 \wedge \cdots \Rightarrow l_2 = r_2$, $\ldots$;
- All these operations are combined possibly yielding several theorems that are applied in parallel.

Mathematical specification (draft): Consider the following:

- a theorem th of the form $\forall x_1 \cdots x_n.\ P \Rightarrow \forall y_1 \cdots y_m.\ l = r$
- a goal g with a subterm t matching l: i.e., there is a substitution σ s.t. $t = l\sigma$

Let:

- p be a propositional atom of g containing t,
- $z_1 \cdots z_p$ be the variables among $x_1, \cdots, x_n, y_1, \cdots, y_m$ that are not instantiated by σ and which do not occur in l.

Then the implicational rewrite of g by th replaces p by:

- $\exists z_1 \cdots z_p.\ P\sigma \wedge p'$, where p' is p where the term t is replaced by $r\sigma$, if p occurs in a positive position (i.e., basically, in the conclusion of an implication and not below a negation);
- $\exists z_1 \cdots z_p.\ P\sigma \Rightarrow p'$, where p' is p where the term t is replaced by $r\sigma$, if p occurs in a negative position (i.e., basically, in the premise of an implication or below a negation);

3 Features to be documented in the following

- `TARGET_REWRITE_TAC`
- implicational conversions