Viewing Proofs

Joe Hurd

ARG Lunch

25 January 2000

1. Goals
2. Concepts
3. Difficulties
4. Results

Goals

1. Users browsing HOL proofs at the right level of detail for their purpose.
2. Avoiding repeatedly invoking costly search tactics by 'rewriting them out of the proof'.
3. Obtaining the primitive inferences that created a theorem.

Concepts

Regard tactics, conversions, tacticals, etc. as rules of inference (i.e., having type `thm list -> thm`). For tactics this is simply the justification function.

Whenever we create a theorem we tag it with the rule of inference (in this expanded sense) that produced it, including the argument theorems.

This creates a proof tree:

thm1 was proved by `STRIP_TAC` which used (produced a subgoal of) thm2 which was proved by `CONJ_TAC` which used thm3 and thm4...

with an option to 'see inside' any (non-primitive) proof step:

thm1 was proved by `STRIP_TAC` which invoked `GEN_TAC` which invoked `GEN`...

Difficulty 1

Naming:

The name of `STRIP_TAC` is "STRIP_TAC".

What is the name of `SPEC_TAC ‘‘x:num‘‘`?

How about
`STRIP_TAC ORELSE SPEC_TAC ‘‘x:num‘‘`?

Decision: names should be as close as possible to what the user typed in.

Difficulty 2

`THEN` Infixes to the Left:

This means

```
STRIP_TAC THEN CONJ_TAC THEN PROVE_TAC []
```

will split (exist on the proof level directly below) as

```
STRIP_TAC THEN CONJ_TAC
```

then

```
PROVE_TAC []
```

This is counter-intuitive!

Decision: re-infixed `THEN` to the right, to produce better splitting of proofs.

Difficulty 3

Unnatural Splitting of the Proof Tree:

`CONJ_TAC` and `SUBGOAL_THEN` always produce 2 subgoals, even if one is relatively trivial.

Mathematics textbooks seem to try and keep proofs linear (probably because they are read in that way) using such devices as 'it is sufficient to prove X since Y'.

Solution: introduce a new tactical `TRIVIAL`, whereby `tac1 TRIVIAL tac2` will apply `tac2` to the first subgoal of `tac1`, hopefully solving it and thus pushing it down to a lower level of the proof tree.

Results

- Good for seeing subgoals that appear in the top-level tactic proof.
- Things become incoherent at lower levels (especially the primitive inferences).
- Major change to the HOL system, just annotating all tactics, conversions, etc. Also require changing proofs so that `THEN` can safely infix to the right, and tactics really need a different type to make tracking names a lot cleaner.
- Future work: add in conversions and rules, and make theorems reference each other properly (i.e., the proper name and an accompanying hyperlink, not just printing the sequent).