Chapter 4

Application and limitations

In this chapter we show how the system we developed for defining inductive predicates in Iris is applicable on a more real world example than MLLs. In the process we show some limitations of the commands and tactics created in this thesis.

In the IPM the total weakest precondition proof rules are not axioms. They are derived from the definition of the total weakest precondition, and, the total weakest precondition is defined in terms of the base Iris logic. This definition is a fixpoint following the procedure in section 3.2thesis.pdf.

In the first section, section 4.1, we show the total weakest precondition can be defined using `eiInd` . Next, in section 4.2 we show what proofs on the total weakest precondition can be done and which can not.

4.1 Defining the total weakest precondition

The total weakest precondition is defined as follows.

Coq

```coq
eiInd
Inductive twp (s : stuckness) :
    coPset -> expr Λ ->
    (val Λ -> iProp Σ) -> iProp Σ :=
  | twp_some E v e1 Φ :
    (|={E}=> Φ v) -∗
    ⌜to_val e1 = Some v⌝ -∗
    twp s E e1 Φ
  | twp_none E e1 Φ :
    (∀ σ1 ns κs nt,
       state_interp σ1 ns κs nt ={E,∅}=∗
       ⌜if s is NotStuck then reducible_no_obs e1 σ1
                         else True⌝ ∗
       ∀ κ e2 σ2 efs,
         ⌜prim_step e1 σ1 κ e2 σ2 efs⌝ ={∅,E}=∗
         ⌜κ = []⌝ ∗
         state_interp σ2 (S ns) κs (length efs + nt) ∗
         twp s E e2 Φ ∗
         [∗ list] ef ∈ efs, twp s ⊤ ef fork_post)
    -∗ ⌜to_val e1 = None⌝
    -∗ twp s E e1 Φ.
```

This definition of the total weakest precondition is mostly more of the same This definition differs in several interesting ways from any inductive predicates we have seen so far. We use two so far unseen Iris connectives, `={_,_}=∗` and `[_ list]`. To achieve this definition of the total weakest precondition one important addition had to be made. `eiInd` has to prove the pre fixpoint function generated from the inductive definition monotone. Luckily we can easily define new instances of `iProper` and `iProperTop` for `={_,_}=∗` and `[_ list]`. Using these instance we are able to fully generate the inductive predicate with all lemmas.

4.2 Proofs using the total weakest precondition