

Chapter 1

Coqand SSReflect

We decided to employ the Small Scale Reflection Extension (**SSReflect**) for the **Coq** proof assistant. The most important factors in this decision were SSREFLECT’s excellent support for finite types, list operations and graphs. SSREFLECT also introduces an alternative scripting language that can often be used to shorten the bookkeeping overhead of proofs considerably.

1.1 Coq

1.2 SSReflect

1.2.1 Finite Types and Ordinals

The most important feature of SSREFLECT for our purpose are finite types. SSREFLECT provides boolean versions of the universal and existential quantifiers on finite types, **forallb** and **existsb**. We can compute the number of elements in a finite type F with $\#|F|$. `enum` gives a list of all items of a finite type. Finite types also come with enumeration functions which provide a consistent ordering. The corresponding functions are `enum.rank` and `enum.val`. The input of `enum.val` and the result of `enum.rank` are ordinals, i.e. values in $[0, \#|F|-1]$. The corresponding type can be written as $1_{\#|F|}$.

1.2.2 Boolean Reflection

SSREFLECT offers boolean reflections for decidable propositions. This allows us to switch back and forth between equivalent boolean and propositional predicates.

1.2.3 Boolean Predicates

We make use of SSREFLECT’s syntax to specify boolean predicates. This allows us to specify predicates in a way that resembles set-theoretic nota-

tion, e.g. $[\text{pred } x \mid \langle \text{boolean expression in } x \rangle]$. Furthermore, we can use the functions `pred1` and `pred0` to specify the singleton predicate and the empty predicate, respectively. The complement of a predicate can be written as $[\text{predC } p]$. The syntax for combining predicates is $[\text{pred? } p1 \ \& \ p2]$, with `?` being replaced with one of `U` (union), `I` (intersection) or `D` (difference). There is also syntax for the preimage of a predicate under a function which can be written as $[\text{preim } f \text{ of } p]$.

There are also applicative (functional) versions of `predC`, `predU`, `predI`, `predD` which are functions that take predicates and return predicates.