

Refleksja, Specyfikacje

12 maja 2009

- Technika dowodów przez „Refleksję”
- Specyfikacje funkcji
- Ekstrakcja programów z (dowodów spełnialności) specyfikacji

Dowodzenie przez „Refleksję”

Refleksja — od *reflexion* — odbicie (np. w lustrze)

⇒ Dowody bezpośrednio przez obliczenie:

- Aby dowodzić $C\ t$ dla $C : T \rightarrow \text{Prop}$
- robimy funkcję $\text{decide_C} : T \rightarrow \text{bool}$
- dowodzimy o niej

`Lemma decide_ok : forall t, decide_C t = true -> C t`

- Aby udowodnić $C\ t$ robimy
`apply decide_ok,`
- dostajemy goal
`decide_C t = true`
- robimy
`reflexivity`
- i już.

Dowodzenie przez refleksje (c.d.)

⇒ Dowody przez obliczenia algebraiczne:

- Aby dowodzić $t=t'$
- robimy „sztuczną dziedzinę” A i funkcję $\text{interp} : A \rightarrow T$
- oraz funkcję $\text{simplify} : A \rightarrow A$
- dowodzimy o niej

```
Lemma simplify_ok : forall t,  
  interp t = interp (simplify t)
```

- Aby udowodnić $t=t'$:
- Zgadujemy odpowiednie a i a' , robimy $\text{change (interp a)=(interp a')}$,
- potem $\text{rewrite simplify_ok}$
- dostajemy $\text{goal (interp (simplify a))=(interp (simplify a))}$
- robimy reflexivity
- i już :)