

Dokazovanje ekvivalenc med programi

Dostikrat si želimo dokazati, da nek program deluje tako, kot želimo. Običajno je to precej zahtevna naloga, saj so programski jeziki nepredvidljivi. Ker pa je Haskell čist jezik, so v njem izrazi enakovredni svojim definicijam, zato lahko ene zamenjamo z drugimi in obratno. Da bomo imeli kaj, s čimer bomo lahko delali, si najprej definirajmo sledeče tri funkcije:

$$[] ++ ys = ys \quad (1)$$

$$(x:xs) ++ ys = x:(xs ++ ys) \quad (2)$$

$$\text{obrni } [] = [] \quad (3)$$

$$\text{obrni } (x:xs) = \text{obrni } xs ++ [x] \quad (4)$$

$$\text{dolzina } [] = 0 \quad (5)$$

$$\text{dolzina } (x:xs) = 1 + \text{dolzina } xs \quad (6)$$

Trd. 1: $\text{obrni } [x] = [x]$

To enostavno trditev dokažemo zgolj z odvijanjem definicij.

$$\begin{aligned} \text{obrni } [x] &= \text{obrni } (x:[]) && \text{ker je } [x] \text{ okrajšava za } x:[] \\ &= [] ++ [x] && \text{po (3)} \\ &= [x] && \text{po (1)} \end{aligned}$$

Trd. 2: $\text{dolzina } (xs ++ ys) = \text{dolzina } xs + \text{dolzina } ys$

Tukaj enostavno odvijanje definicij ne bo pomagalo, saj izraz $\text{dolzina } (xs ++ ys)$ ne ustreza ne levi ne desni strani nobene od zgoraj naštetih definicij. Namesto tega uporabimo načelo indukcije za sezname:

$$P([]) \wedge (\forall x, xs. P(xs) \Rightarrow P(x:xs)) \implies \forall ys. P(ys)$$

Torej, lastnost P velja za vse sezname ys , kadar (1) velja za prazen seznam $[]$ in (2) velja za sestavljen seznam $x:xs$ ob predpostavki, da velja za xs . Načelo indukcije je podobno načelu indukcije za naravna števila:

$$P(0) \wedge (\forall m. P(m) \Rightarrow P(m^+)) \implies \forall n. P(n)$$

Torej, lastnost P velja za vsa naravna števila n , kadar (1) velja za 0 in (2) velja za naslednika m^+ ob predpostavki, da velja za m .

Izjavo dokažemo z indukcijo na levi seznam. Indukcija poteka v dveh korakih:

Osnovni korak

V osnovnem koraku pokažemo, da enakost velja, kadar je levi seznam prazen, torej oblike []:

$$\begin{aligned} \text{dolzina } ([] ++ \text{ys}) &= \text{dolzina } \text{ys} && \text{po (1)} \\ &= 0 + \text{dolzina } \text{ys} && \text{po Peanovih aksiomih} \\ &= \text{dolzina } [] + \text{dolzina } \text{ys} && \text{po (5)} \end{aligned}$$

Indukcijski korak

V indukcijskem koraku pokažemo, da enakost velja za sestavljeni seznam $x:xs$ ob predpostavki, da enakost velja za seznam xs :

$$\begin{aligned} \text{dolzina } ((x:xs) ++ \text{ys}) &= \text{dolzina } (x:(xs ++ \text{ys})) && \text{po (2)} \\ &= 1 + \text{dolzina } (xs ++ \text{ys}) && \text{po (6)} \\ &= 1 + (\text{dolzina } xs + \text{dolzina } \text{ys}) && \text{po induksijski prepostavki} \\ &= (1 + \text{dolzina } xs) + \text{dolzina } \text{ys} && \text{po Peanovih aksiomih} \\ &= \text{dolzina } (x:xs) + \text{dolzina } \text{ys} && \text{po (6)} \end{aligned}$$

Trd. 3: $xs ++ [] = xs$

Po (1) vemo, da je $[] ++ xs = xs$, torej je $[]$ leva enota za $++$. To, da je $[]$ tudi desna enota, pa ni samoumevno — za dokaz uporabimo indukcijo.

Osnovni korak

Po (1) velja $[] ++ [] = []$, kar dokaže osnovni korak.

Indukcijski korak

Prepostavimo, da velja $xs ++ [] = xs$. Tedaj velja

$$\begin{aligned} (x:xs) ++ [] &= x:(xs ++ []) && \text{po (2)} \\ &= x:xs && \text{po induksijski prepostavki,} \end{aligned}$$

kar zaključi tudi indukcijski korak.

Trd. 4: $xs ++ (ys ++ zs) = (xs ++ ys) ++ zs$

Operacija stikanja seznamov $++$ je tudi asociativna, kar dokažemo z indukcijo na xs . Če zapišete dokaz asociativnosti seštevanja, lahko vidite, da poteka podobno, le da se namesto $[]$ pojavlja 0, namesto $x:xs$ pa naslednik n^+ .

Osnovni korak

$$\begin{aligned} [] ++ (ys ++ zs) &= ys ++ zs && \text{po (1)} \\ &= ([] ++ ys) ++ zs && \text{po (1)} \end{aligned}$$

Indukcijski korak

Prepostavimo, da velja $xs ++ (ys ++ zs) = (xs ++ ys) ++ zs$. Tedaj velja

$$\begin{aligned} (x:xs) ++ (ys ++ zs) &= x:(xs ++ (ys ++ zs)) && \text{po (2)} \\ &= x:((xs ++ ys) ++ zs) && \text{po indukcijski predpostavki} \\ &= (x:(xs ++ ys)) ++ zs && \text{po (2)} \\ &= ((x:xs) ++ ys) ++ zs && \text{po (2)} \end{aligned}$$

Trd. 5: $\text{obrni } (xs ++ ys) = \text{obrni } ys ++ \text{obrni } xs$

Osnovni korak

$$\begin{aligned} \text{obrni } ([] ++ ys) &= \text{obrni } ys && \text{po (1)} \\ &= \text{obrni } ys ++ [] && \text{po trditvi 3} \\ &= \text{obrni } ys ++ \text{obrni } [] && \text{po (3)} \end{aligned}$$

Indukcijski korak

$$\begin{aligned} \text{obrni } ((x:xs) ++ ys) &= \text{obrni } (x:(xs ++ ys)) && \text{po (2)} \\ &= \text{obrni } (xs ++ ys) ++ [x] && \text{po (4)} \\ &= (\text{obrni } ys ++ \text{obrni } xs) ++ [x] && \text{po indukcijski predpostavki} \\ &= \text{obrni } ys ++ (\text{obrni } xs ++ [x]) && \text{po trditvi 4} \\ &= \text{obrni } ys ++ \text{obrni } (x:xs) && \text{po (4)} \end{aligned}$$

Trd. 6: $\text{obrni } (\text{obrni } xs) = xs$

Na kvizu.

Trd. 7: $\text{dolzina } (\text{obrni } xs) = \text{dolzina } xs$

Domača naloga.