Dimostrazione di proprietà di funzioni sulle liste

Luca Padovani
Linguaggi e Paradigmi di Programmazione

principio di induzione sulle liste finite

- **ogni** lista finita è costruita a partire dalla lista vuota [] e un numero **finito** di applicazioni del costruttore : (cons)

principio di induzione sulle liste finite

Data una proprietà $P(xs)$ delle liste, se

- $P([])$ e
- $P(xs)$ implica $P(x : xs)$ per ogni x e xs,

allora $P(xs)$ per ogni lista finita xs.

- come nel caso dell'induzione sui numeri naturali il principio si può generalizzare a tutte le liste **più corte** di quella considerata per dimostrare il caso induttivo

alcune funzioni notevoli sulle liste

```
length :: [a] → Int
length []         = 0
length (_ : xs) = 1 + length xs
```

```
(++) :: [a] → [a] → [a]
(++) []       ys = ys
(++) (x : xs) ys = x : (++) xs ys
```

```
reverse :: [a] → [a]
reverse []       = []
reverse (x : xs) = reverse xs ++ [x]
```

Seguono alcune proprietà che vorremmo dimostrare

1. $\forall xs, ys : \texttt{length}\,(xs +\!\!+\, ys) = \texttt{length}\,xs + \texttt{length}\,ys$
2. $\forall xs, ys, zs : xs +\!\!+\, (ys +\!\!+\, zs) = (xs +\!\!+\, ys) +\!\!+\, zs$
3. $\forall xs, ys : \texttt{reverse}\,(xs +\!\!+\, ys) = \texttt{reverse}\,ys +\!\!+\, \texttt{reverse}\,xs$

$$P(xs) \stackrel{\text{def}}{=} \texttt{length}\ (xs \mathbin{+\!\!+} ys) = \texttt{length}\ xs + \texttt{length}\ ys$$

$P([])$ lato sinistro

$$\begin{aligned}
&\texttt{length}\ ([] \mathbin{+\!\!+} ys) \\
&\quad = \texttt{length}\ ys && (\texttt{++.1})
\end{aligned}$$

$P([])$ lato destro

$$\begin{aligned}
&\texttt{length}\ [] + \texttt{length}\ ys \\
&\quad = 0 + \texttt{length}\ ys && (\texttt{length.1}) \\
&\quad = \texttt{length}\ ys && (\text{proprietà di } +)
\end{aligned}$$

$P(xs) \Rightarrow P(x : xs)$ lato sinistro

$$\begin{aligned}
&\texttt{length}\ ((x : xs) \mathbin{+\!\!+} ys) \\
&\quad = \texttt{length}\ (x : (xs \mathbin{+\!\!+} ys)) && (\texttt{++.2}) \\
&\quad = 1 + \texttt{length}\ (xs \mathbin{+\!\!+} ys) && (\texttt{length.2}) \\
&\quad = 1 + \texttt{length}\ xs + \texttt{length}\ ys && (\text{ipotesi induttiva})
\end{aligned}$$

$P(xs) \Rightarrow P(x : xs)$ lato destro

$$\begin{aligned}
&\texttt{length}\ (x : xs) + \texttt{length}\ ys \\
&\quad = (1 + \texttt{length}\ xs) + \texttt{length}\ ys && (\texttt{length.1}) \\
&\quad = 1 + \texttt{length}\ xs + \texttt{length}\ ys && (\text{proprietà di } +)
\end{aligned}$$

$$P(xs) \overset{\text{def}}{=} \forall ys, zs : xs +\!\!+ (ys +\!\!+ zs) = (xs +\!\!+ ys) +\!\!+ zs$$

$P([])$

$$\begin{aligned} & [] +\!\!+ (ys +\!\!+ zs) \\ & \quad = ys +\!\!+ zs && (\texttt{++.1}) \\ & \quad = ([] +\!\!+ ys) +\!\!+ zs && (\texttt{++.1}) \end{aligned}$$

$P(xs) \Rightarrow P(x : xs)$ — lato sinistro

$$\begin{aligned} & (x : xs) +\!\!+ (ys +\!\!+ zs) \\ & \quad = x : (xs +\!\!+ (ys +\!\!+ zs)) && (\texttt{++.2}) \\ & \quad = x : ((xs +\!\!+ ys) +\!\!+ zs) && (\text{ipotesi induttiva}) \end{aligned}$$

$P(xs) \Rightarrow P(x : xs)$ — lato destro

$$\begin{aligned} & ((x : xs) +\!\!+ ys) +\!\!+ zs \\ & \quad = (x : (xs +\!\!+ ys)) +\!\!+ zs && (\texttt{++.2}) \\ & \quad = x : ((xs +\!\!+ ys) +\!\!+ zs) && (\texttt{++.2}) \end{aligned}$$

$$P(xs) \stackrel{\text{def}}{=} \forall ys : \texttt{reverse}\ (xs +\!\!+\ ys) = \texttt{reverse}\ ys +\!\!+\ \texttt{reverse}\ xs$$

$P([])$ lato sinistro

$$\begin{aligned} &\texttt{reverse}\ ([] +\!\!+\ ys) \\ &\quad = \texttt{reverse}\ ys && (\texttt{++.1}) \end{aligned}$$

$P([])$ lato destro

$$\begin{aligned} &\texttt{reverse}\ ys +\!\!+\ \texttt{reverse}\ [] \\ &\quad = \texttt{reverse}\ ys +\!\!+\ [] && (\texttt{reverse.1}) \\ &\quad = \texttt{reverse}\ ys && (\text{proprietà di } +\!\!+ \text{ da dimostrare!}) \end{aligned}$$

$P(x : xs)$ lato sinistro

$$\begin{aligned} &\texttt{reverse}\ ((x : xs) +\!\!+\ ys) \\ &\quad = \texttt{reverse}\ (x : (xs +\!\!+\ ys)) && (\texttt{++.2}) \\ &\quad = \texttt{reverse}\ (xs +\!\!+\ ys) +\!\!+\ [x] && (\texttt{reverse.2}) \\ &\quad = (\texttt{reverse}\ ys +\!\!+\ \texttt{reverse}\ xs) +\!\!+\ [x] && (\text{ipotesi induttiva}) \end{aligned}$$

$P(x : xs)$ lato destro

$$\begin{aligned} &\texttt{reverse}\ ys +\!\!+\ \texttt{reverse}\ (x : xs) \\ &\quad = \texttt{reverse}\ ys +\!\!+\ (\texttt{reverse}\ xs +\!\!+\ [x]) && (\texttt{reverse.2}) \\ &\quad = (\texttt{reverse}\ ys +\!\!+\ \texttt{reverse}\ xs) +\!\!+\ [x] && (\text{associatività di } +\!\!+) \end{aligned}$$

`reverse` efficiente

```
rev :: [a] → [a]
rev xs = shunt xs []
  where
    shunt []       ys = ys
    shunt (x : xs) ys = shunt xs (x : ys)
```

`rev` è corretta?

- $\forall xs : \texttt{rev}\ xs = \texttt{reverse}\ xs$

$P(xs) \stackrel{\text{def}}{=} \texttt{rev}\ xs = \texttt{reverse}\ xs$ (primo tentativo)

$P([])$

$$
\begin{aligned}
&\texttt{rev}\ [] \\
&\quad = \texttt{shunt}\ []\ [] && (\texttt{rev.1}) \\
&\quad = [] && (\texttt{shunt.1}) \\
&\quad = \texttt{reverse}\ [] && (\texttt{reverse.1})
\end{aligned}
$$

$P(x : xs)$ lato sinistro

$$
\begin{aligned}
&\texttt{rev}\ (x : xs) \\
&\quad = \texttt{shunt}\ (x : xs)\ [] && (\texttt{rev.1}) \\
&\quad = \texttt{shunt}\ xs\ [x] && (\texttt{shunt.2})
\end{aligned}
$$

$P(x : xs)$ lato destro

$$
\begin{aligned}
&\texttt{reverse}\ (x : xs) \\
&\quad = \texttt{reverse}\ xs \mathbin{+\!\!+} [x] && (\texttt{reverse.2}) \\
&\quad = \texttt{rev}\ xs \mathbin{+\!\!+} [x] && \text{(ipotesi induttiva)} \\
&\quad = \texttt{shunt}\ xs\ [] \mathbin{+\!\!+} [x] && (\texttt{rev.1})
\end{aligned}
$$

- non si riesce a procedere, occorre un risultato più generale

$P(xs) \overset{\text{def}}{=} \forall ys : \texttt{shunt}\ xs\ ys = \texttt{reverse}\ xs \mathbin{+\!\!+} ys$

$P([])$

$$\begin{aligned}
&\texttt{shunt}\ []\ ys \\
&\quad = ys && (\texttt{shunt.1}) \\
&\quad = [] \mathbin{+\!\!+} ys && (\texttt{append.1}) \\
&\quad = \texttt{reverse}\ [] \mathbin{+\!\!+} ys && (\texttt{reverse.1})
\end{aligned}$$

$P(x : xs)$ lato sinistro

$$\begin{aligned}
&\texttt{shunt}\ (x : xs)\ ys \\
&\quad = \texttt{shunt}\ xs\ (x : ys) && (\texttt{shunt.2}) \\
&\quad = \texttt{reverse}\ xs \mathbin{+\!\!+} (x : ys) && (\text{ipotesi induttiva})
\end{aligned}$$

$P(x : xs)$ lato destro

$$\begin{aligned}
&\texttt{reverse}\ (x : xs) \mathbin{+\!\!+} ys \\
&\quad = (\texttt{reverse}\ xs \mathbin{+\!\!+} [x]) \mathbin{+\!\!+} ys && (\texttt{reverse.2}) \\
&\quad = \texttt{reverse}\ xs \mathbin{+\!\!+} ([x] \mathbin{+\!\!+} ys) && (\text{associatività di } \mathbin{+\!\!+}) \\
&\quad = \texttt{reverse}\ xs \mathbin{+\!\!+} (x : ([] \mathbin{+\!\!+} ys)) && (\texttt{append.2}) \\
&\quad = \texttt{reverse}\ xs \mathbin{+\!\!+} (x : ys) && (\texttt{append.1})
\end{aligned}$$

correttezza di `rev`

$$
\begin{aligned}
&\texttt{rev}\ xs \\
&\quad = \texttt{shunt}\ xs\ [] && (\texttt{rev.1}) \\
&\quad = \texttt{reverse}\ xs \mathbin{+\!\!+} [] && \text{(dimostrato in precedenza)} \\
&\quad = \texttt{reverse}\ xs && \text{(proprietà di } \mathbin{+\!\!+}\text{, vedi esercizi)}
\end{aligned}
$$

approccio top-down alla dimostrazione di proprietà

```
filter :: (a → Bool) → [a] → [a]
filter _ [] = []
filter f (x : xs) | f x       = x : filter f xs
                  | otherwise = filter f xs
```

Problema

- Dimostrare la seguente proprietà di `filter`

$$\forall f, xs : \texttt{filter}\, f\ (\texttt{reverse}\, xs) = \texttt{reverse}\ (\texttt{filter}\, f\ xs)$$

- Non è facile immaginare quali proprietà ausiliarie ci serviranno
- Iniziamo la dimostrazione e annotiamo i **lemmi** che servono
- Successivamente dimostriamo i lemmi

$$P(xs) \stackrel{\text{def}}{=} \forall f : \texttt{filter}\, f\, (\texttt{reverse}\, xs) = \texttt{reverse}\, (\texttt{filter}\, f\, xs)$$

$P([])$

$$\begin{aligned}
&\texttt{filter}\, f\, (\texttt{reverse}\, [])\\
&\quad = \texttt{filter}\, f\, [] && (\texttt{reverse.1})\\
&\quad = [] && (\texttt{filter.1})\\
&\quad = \texttt{reverse}\, [] && (\texttt{reverse.1})\\
&\quad = \texttt{reverse}\, (\texttt{filter}\, f\, []) && (\texttt{filter.1})
\end{aligned}$$

$P(xs) \Rightarrow P(x : xs)$

$$\begin{aligned}
&\texttt{filter}\, f\, (\texttt{reverse}\, (x : xs))\\
&\quad = \texttt{filter}\, f\, (\texttt{reverse}\, xs \mathbin{+\!\!+} [x]) && (\texttt{reverse.2})\\
&\quad = \texttt{filter}\, f\, (\texttt{reverse}\, xs) \mathbin{+\!\!+} \texttt{filter}\, f\, [x] && (\text{lemma 1})\\
&\quad = \texttt{reverse}\, (\texttt{filter}\, f\, xs) \mathbin{+\!\!+} \texttt{filter}\, f\, [x] && (\text{ipotesi induttiva})\\
&\quad = \texttt{reverse}\, (\texttt{filter}\, f\, xs) \mathbin{+\!\!+} \texttt{reverse}\, (\texttt{filter}\, f\, [x]) && (\text{lemma 2})\\
&\quad = \texttt{reverse}\, (\texttt{filter}\, f\, [x] \mathbin{+\!\!+} \texttt{filter}\, f\, xs) && (\text{dimostrato in precedenza})\\
&\quad = \texttt{reverse}\, (\texttt{filter}\, f\, ([x] \mathbin{+\!\!+} xs)) && (\text{lemma 1})\\
&\quad = \texttt{reverse}\, (\texttt{filter}\, f\, (x : ([] \mathbin{+\!\!+} xs))) && (\texttt{append.2})\\
&\quad = \texttt{reverse}\, (\texttt{filter}\, f\, (x : xs)) && (\texttt{append.1})
\end{aligned}$$

esercizi

Dimostrare le seguenti proprietà

1. $\forall xs : xs +\!\!+ [] = xs$
2. $\forall xs : \texttt{length}\ (\texttt{reverse}\ xs) = \texttt{length}\ xs$
3. $\forall xs : \texttt{reverse}\ (\texttt{reverse}\ xs) = xs$
4. $\forall xs : \texttt{sum}\ (\texttt{reverse}\ xs) = \texttt{sum}\ xs$
5. $\forall xs, ys : \texttt{sum}\ (xs +\!\!+ ys) = \texttt{sum}\ xs + \texttt{sum}\ ys$

```haskell
sublist :: Eq a => [a] -> [a] -> Bool
sublist [] _   = True
sublist _   [] = False
sublist (x : xs) (y : ys) | x == y = sublist xs ys
sublist xs (_ : ys) = sublist xs ys
```

6. $\forall f, xs : \texttt{sublist}\ (\texttt{filter}\ f\ xs)\ xs = \texttt{True}$ IMP

principio di induzione su tipi algebrici

```
data Tree a = Leaf | Branch a (Tree a) (Tree a)
```

principio di induzione sugli alberi

Data una proprietà $P(t)$ degli alberi, se

- $P(\texttt{Leaf})$ e
- $P(t_1) \wedge P(t_2)$ implica $P(\texttt{Branch}\ x\ t_1\ t_2)$ per ogni x, t_1 e t_2

allora $P(t)$ per ogni albero (finito) t.

```
leaves :: Tree a → Int
leaves Leaf = 1
leaves (Branch _ t₁ t₂) = leaves t₁ + leaves t₂
```

```
branches :: Tree a → Int
branches Leaf = 0
branches (Branch _ t₁ t₂) = 1 + branches t₁ + branches t₂
```

- $\forall t : \texttt{leaves}\ t = 1 + \texttt{branches}\ t$

$P(t) = \texttt{leaves}\ t = 1 + \texttt{branches}\ t$

$P(\texttt{Leaf})$

$$
\begin{aligned}
&\texttt{leaves Leaf} \\
&\quad = 1 && (\texttt{leaves.1}) \\
&\quad = 1 + 0 && (\text{proprietà di } +) \\
&\quad = 1 + \texttt{branches Leaf} && (\text{branches.1})
\end{aligned}
$$

$P(t_1) \wedge P(t_2) \Rightarrow P(\texttt{Branch}\ x\ t_1\ t_2)$

$$
\begin{aligned}
&\texttt{leaves}\ (\texttt{Branch}\ x\ t_1\ t_2) \\
&\quad = \texttt{leaves}\ t_1 + \texttt{leaves}\ t_2 && (\texttt{leaves.2}) \\
&\quad = (1 + \texttt{branches}\ t_1) + (1 + \texttt{branches}\ t_2) && (\text{ipotesi induttiva}) \\
&\quad = 1 + (1 + \texttt{branches}\ t_1 + \texttt{branches}\ t_2) && (\text{proprietà di } +) \\
&\quad = 1 + \texttt{branches}\ (\texttt{Branch}\ x\ t_1\ t_2) && (\texttt{branches.2})
\end{aligned}
$$

esercizi

```
depth :: Tree a → Int
depth Leaf = 0
depth (Branch _ t₁ t₂) = 1 + max (depth t₁) (depth t₂)
```

```
elements :: Tree a → [a]
elements Leaf = []
elements (Branch x t₁ t₂) = x:(elements t₁ ++ elements t₂)
```

1. $\forall t : \texttt{depth}\ t \leq \texttt{leaves}\ t$
2. $\forall t : \texttt{length}\ (\texttt{elements}\ t) = \texttt{branches}\ t$
3. $\forall t : \texttt{branches}\ t \leq 2\texttt{\^{}depth}\ t - 1$