[redacted]strazione di proprietà di funzioni su numeri interi

[redacted]uca Padovani
Linguaggi e Paradigmi di Programmazione

correttezza e verifica di proprietà di funzioni

Problemi

- ~~date una funzione e una specifica di ciò che la funzione dovrebbe calcolare, la funzione è **corretta** rispetto alla specifica?~~
- ~~date due funzioni (per es. una ovviamente corretta ma inefficiente, l'altra efficiente ma più complessa da capire), sono **equivalenti**?~~

Vari approcci, tra cui:

- Test
  - più facile (specialmente se il linguaggio non è imperativo)
  - analisi non esaustiva (possono esserci errori in casi non considerati)
- Dimostrazione
  - più difficile (specialmente se il linguaggio è imperativo)
  - analisi esaustiva

esempio

Che funzione è?

```
foo :: Int → Int → Int → Int
foo x y z | y < x     = foo y x z
          | z < y     = foo x z y
          | otherwise = z
```

Una proprietà che ci aspettiamo da `foo`. Sarà vera?

1. $\forall x, y, z : \texttt{foo}\; x\; y\; z = \max\{x, y, z\}$

- possiamo fare dei **test**, ma questi saranno sempre in numero finito
- possiamo cercare una **dimostrazione**

Dimostrazione per casi

- Siccome i numeri sono infiniti (o "tanti"), non possiamo verificare il comportamento di `foo` per **tutti** i possibili argomenti
- Siccome l'ordine tra numeri è **totale**, possiamo considerare un numero **finito** di casi complessivamente **esaustivi**

1. $x \leq y \leq z \quad \Rightarrow \quad \texttt{foo}\ x\ y\ z = z$
2. $x \leq z < y \quad \Rightarrow \quad \texttt{foo}\ x\ y\ z = \texttt{foo}\ x\ z\ y = y$
3. $y < x \leq z \quad \Rightarrow \quad \texttt{foo}\ x\ y\ z = \texttt{foo}\ y\ x\ z = z$
4. $y \leq z < x \quad \Rightarrow \quad \texttt{foo}\ x\ y\ z = \texttt{foo}\ y\ x\ z = \texttt{foo}\ y\ z\ x = x$
5. $z < x \leq y \quad \Rightarrow \quad \texttt{foo}\ x\ y\ z = \texttt{foo}\ x\ z\ y = \texttt{foo}\ z\ x\ y = y$
6. $z < y < x \quad \Rightarrow \quad \texttt{foo}\ x\ y\ z = \texttt{foo}\ y\ x\ z = \texttt{foo}\ y\ z\ x = \texttt{foo}\ z\ y\ x = x$

Nota

- Non essendoci lo **stato**, il codice del programma è tutto quello che serve per ragionare su queste equivalenze

principio di induzione sui numeri naturali

- l'approccio esaustivo è plausibile se ci sono solo finiti casi da considerare
- il principio di induzione consente di dimostrare che una proprietà vale per un insieme **infinito** di casi

principio di induzione sui numeri naturali

Data una proprietà $P(n)$ dei numeri naturali, se

- $P(0)$ e
- $P(n)$ implica $P(n+1)$ per ogni $n \in \mathbb{N}$,

allora $P(n)$ per ogni $n \in \mathbb{N}$.

esponenziale

```
exp :: Int → Int → Int
exp _ 0 = 1
exp x n = x * exp x (n - 1)
```

Seguono alcune proprietà che vorremmo dimostrare

1. $\forall x, m \geq 0, n \geq 0 : \texttt{exp}\ x\ (m + n) = \texttt{exp}\ x\ m * \texttt{exp}\ x\ n$
2. $\forall x, n \geq 0 : \texttt{exp}\ (x * x)\ n = \texttt{exp}\ x\ n * \texttt{exp}\ x\ n$

$P(m) \stackrel{\text{def}}{=} \forall x, n \geq 0 : \texttt{exp}\ x\ (m+n) = \texttt{exp}\ x\ m * \texttt{exp}\ x\ n$

$P(0)$ lato sinistro

$\texttt{exp}\ x\ (0+n)$

$= \texttt{exp}\ x\ n$ (proprietà di $+$)

$P(0)$ lato destro

$\texttt{exp}\ x\ 0 * \texttt{exp}\ x\ n$

$= 1 * \texttt{exp}\ x\ n$ $(\texttt{exp.1})$

$= \texttt{exp}\ x\ n$ (proprietà di $*$)

$P(m-1) \Rightarrow P(m)$ per ogni $m > 0$ lato sinistro

$\texttt{exp}\ x\ (m+n)$

$= x * \texttt{exp}\ x\ ((m+n)-1)$ $(\texttt{exp.2})$

$= x * \texttt{exp}\ x\ ((m-1)+n)$ (proprietà di $+$ e $-$)

$= x * (\texttt{exp}\ x\ (m-1) * \texttt{exp}\ x\ n)$ (ipotesi induttiva)

$P(m-1) \Rightarrow P(m)$ per ogni $m > 0$ lato destro

$\texttt{exp}\ x\ m \times \texttt{exp}\ x\ n$

$= (x * \texttt{exp}\ x\ (m-1)) * \texttt{exp}\ x\ n$ $(\texttt{exp.2})$

$= x * (\texttt{exp}\ x\ (m-1) * \texttt{exp}\ x\ n)$ (proprietà di $*$)

$$P(n) \stackrel{\text{def}}{=} \forall x : \texttt{exp}\ (x * x)\ n = \texttt{exp}\ x\ n * \texttt{exp}\ x\ n$$

$P(0)$ lato sinistro

$\texttt{exp}\ (x * x)\ 0 = 1$ $(\texttt{exp.1})$

$P(0)$ lato destro

$\texttt{exp}\ x\ 0 * \texttt{exp}\ x\ 0$

$= 1 * 1$ $(\texttt{exp.1})$

$= 1$ (proprietà di $*$)

$P(n-1) \Rightarrow P(n)$ per ogni $n > 0$ lato sinistro

$\texttt{exp}\ (x * x)\ n$

$= (x * x) * \texttt{exp}\ (x * x)\ (n-1)$ $(\texttt{exp.2})$

$= (x * x) * (\texttt{exp}\ x\ (n-1) * \texttt{exp}\ x\ (n-1))$ (ipotesi induttiva)

$P(n-1) \Rightarrow P(n)$ per ogni $n > 0$ lato destro

$\texttt{exp}\ x\ n * \texttt{exp}\ x\ n$

$= (x * \texttt{exp}\ x\ (n-1)) * (x * \texttt{exp}\ x\ (n-1))$ $(\texttt{exp.2})$

$= (x * x) * (\texttt{exp}\ x\ (n-1) * \texttt{exp}\ x\ (n-1))$ (proprietà di $*$)

esponenziale efficiente

```
fexp :: Int → Int → Int
fexp x n | n == 0    = 1
         | even n    = fexp (x * x) (n `div` 2)
         | otherwise = x * fexp x (n - 1)
```

- `fexp` ed `exp` sono equivalenti?

principio di induzione forte

Data una proprietà $P(n)$ dei numeri naturali, se

- $(\forall m < n : P(m)) \Rightarrow P(n)$ per ogni $n \in \mathbb{N}$

allora $P(n)$ per ogni $n \in \mathbb{N}$.

- si può dimostrare che il principio di induzione forte è equivalente al principio di induzione, ma a volte è più comodo da usare perché fornisce un'ipotesi induttiva **più forte**.

$P(n) \stackrel{\text{def}}{=} \forall x : \texttt{fexp}\ x\ n = \texttt{exp}\ x\ n$

$P(0)$

$$
\begin{aligned}
&\texttt{fexp}\ x\ 0 \\
&\quad = 1 && (\texttt{fexp.1}) \\
&\quad = \texttt{exp}\ x\ 0 && (\texttt{exp.1})
\end{aligned}
$$

$(\forall m < n : P(m)) \Rightarrow P(n)$ quando $n > 0$ è pari

$$
\begin{aligned}
&\texttt{fexp}\ x\ n \\
&\quad = \texttt{fexp}\ (x * x)\ (n/2) && (\texttt{fexp.2}) \\
&\quad = \texttt{exp}\ (x * x)\ (n/2) && \text{(ipotesi induttiva)} \\
&\quad = \texttt{exp}\ x\ (n/2) * \texttt{exp}\ x\ (n/2) && \text{(dimostrato in precedenza)} \\
&\quad = \texttt{exp}\ x\ (n/2 + n/2) && \text{(dimostrato in precedenza)} \\
&\quad = \texttt{exp}\ x\ n && \text{(proprietà di / e +)}
\end{aligned}
$$

$(\forall m < n : P(m)) \Rightarrow P(n)$ quando $n > 0$ è dispari

$$
\begin{aligned}
&\texttt{fexp}\ x\ n \\
&\quad = x * \texttt{fexp}\ x\ (n - 1) && (\texttt{fexp.3}) \\
&\quad = x * \texttt{exp}\ x\ (n - 1) && \text{(ipotesi induttiva)} \\
&\quad = \texttt{exp}\ x\ n && (\texttt{exp.2})
\end{aligned}
$$

sequenza di Fibonacci

```
fibo :: Int → Int
fibo 0 = 0
fibo 1 = 1
fibo k = fibo (k - 2) + fibo (k - 1)
```

```
ffibo :: Int → Int
ffibo = aux 0 1
  where
    aux m _ 0 = m
    aux m n k = aux n (m + n) (k - 1)
```

- cosa si può dire di `ffibo`? È equivalente a `fibo`?

$$P(k) \stackrel{\text{def}}{=} \forall n : \mathtt{aux}\ (\mathtt{fibo}\ n)\ (\mathtt{fibo}\ (n+1))\ k = \mathtt{fibo}\ (n+k)$$

$P(0)$

$$\begin{aligned}
&\mathtt{aux}\ (\mathtt{fibo}\ n)\ (\mathtt{fibo}\ (n+1))\ 0 \\
&\quad = \mathtt{fibo}\ n && (\mathtt{aux.1}) \\
&\quad = \mathtt{fibo}\ (n+0) && (\text{proprietà di } +)
\end{aligned}$$

$P(k-1) \Rightarrow P(k)$ quando $k > 0$

$$\begin{aligned}
&\mathtt{aux}\ (\mathtt{fibo}\ n)\ (\mathtt{fibo}\ (n+1))\ k \\
&\quad = \mathtt{aux}\ (\mathtt{fibo}\ (n+1))\ (\mathtt{fibo}\ n + \mathtt{fibo}\ (n+1))\ (k-1) && (\mathtt{aux.2}) \\
&\quad = \mathtt{aux}\ (\mathtt{fibo}\ (n+1))\ (\mathtt{fibo}\ (n+2))\ (k-1) && (\mathtt{fibo.3}) \\
&\quad = \mathtt{fibo}\ (n+1+k-1) && (\text{ipotesi induttiva}) \\
&\quad = \mathtt{fibo}\ (n+k) && (\text{proprietà di } +)
\end{aligned}$$

$P(k) \stackrel{\text{def}}{=} \texttt{ffibo}\ k = \texttt{fibo}\ k$

$$
\begin{aligned}
& \texttt{ffibo}\ k \\
& \quad = \texttt{aux}\ 0\ 1\ k && (\texttt{ffibo.1}) \\
& \quad = \texttt{aux}\ (\texttt{fibo}\ 0)\ (\texttt{fibo}\ 1)\ k && (\texttt{fibo.1}\ \text{e}\ \texttt{fibo.2}) \\
& \quad = \texttt{fibo}\ (0 + k) && (\text{dimostrato in precedenza}) \\
& \quad = \texttt{fibo}\ k && (\text{proprietà di } +)
\end{aligned}
$$

Esercizi

```
log :: Int → Int
log 1 = 0
log n = 1 + log (n `div` 2)

div :: Int → Int → Int
div m n | m < n      = 0
        | otherwise = 1 + div (m - n) n

rem :: Int → Int → Int
rem m n | m < n      = m
        | otherwise = rem (m - n) n
```

Dimostrare le proprietà:

1. $\forall n > 0 : \texttt{log}\,(2 * n) = 1 + \texttt{log}\, n$
2. $\forall n \geq 0 : \texttt{log}\,(\texttt{exp}\ 2\ n) = n$
3. $\forall m \geq 0, n > 0 : 0 \leq \texttt{rem}\ m\ n < n$
4. $\forall m \geq 0, n > 0 : n * \texttt{div}\ m\ n + \texttt{rem}\ m\ n = m$

Soluzione esercizio 4

- Uso l'induzione forte su m per dimostrare la proprietà $P(m,n) = n * \texttt{div}\ m\ n + \texttt{rem}\ m\ n = m$ per ogni $m \geq 0$ e $n > 0$.
- Viste le definizioni di `div` e `rem` distinguo due casi.

$(\forall k < m : P(k,n)) \Rightarrow P(m,n)$ quando $m < n$

$$
\begin{aligned}
& n * \texttt{div}\ m\ n + \texttt{rem}\ m\ n \\
& \quad = n * 0 + m && (\texttt{div.1} \text{ e } \texttt{rem.1}) \\
& \quad = m && (\text{prop. di } + \text{ e } *)
\end{aligned}
$$

$(\forall k < m : P(k,n)) \Rightarrow P(m,n)$ quando $m \geq n$

$$
\begin{aligned}
& n * \texttt{div}\ m\ n + \texttt{rem}\ m\ n \\
& \quad = n * (1 + \texttt{div}\ (m-n)\ n) + \texttt{rem}\ (m-n)\ n && (\texttt{div.2} \text{ e } \texttt{rem.2}) \\
& \quad = (n * 1 + n * \texttt{div}\ (m-n)\ n) + \texttt{rem}\ (m-n)\ n && (\text{distr. di } * \text{ su } +) \\
& \quad = (n + n * \texttt{div}\ (m-n)\ n) + \texttt{rem}\ (m-n)\ n && (\text{prop. di } * \text{ e } 1) \\
& \quad = n + (n * \texttt{div}\ (m-n)\ n + \texttt{rem}\ (m-n)\ n) && (\text{assoc. di } +) \\
& \quad = n + (m-n) && (\text{ip. ind. poiché } m-n < m) \\
& \quad = m && (\text{prop. di } + \text{ e } -)
\end{aligned}
$$