A Proof Puzzle: Solution

Ralf Hinze

Computing Laboratory, University of Oxford
Wolfson Building, Parks Road, Oxford, OX1 3QD, England
ralf.hinze@comlab.ox.ac.uk
http://www.comlab.ox.ac.uk/ralf.hinze/

June 2008

Background: Streams

$$\text{data Stream a} = \text{Cons a (Stream a)}$$

$$\text{nat} = \text{Cons 0 (map (+1) nat)}$$

$$\text{nat} = \text{iterate (+1) 0}$$

Background: Infinite trees

$$\text{data Tree a} = \text{Node (Tree a) a (Tree a)}$$

$$\text{nat} = \text{Node 0 (map } (\lambda \text{i} \rightarrow 2 * \text{i} + 1) \text{ nat) (map } (\lambda \text{i} \rightarrow 2 * \text{i} + 2) \text{ nat)}$$

$$\text{nat} = \text{branch } (\lambda \text{i} \rightarrow 2 * \text{i} + 1) \ (\lambda \text{i} \rightarrow 2 * \text{i} + 2) \ 0$$

ϵ

0 1

00 10 01 11

000 100 010 110 001 101 011 111

ϵ

0 1

00 01 10 11

000 001 010 011 100 101 110 111

Lemma

Define:

$$\mathtt{a} \lhd \mathtt{x} = \mathbf{map}\ ([\mathtt{a}] +\!\!+)\ \mathtt{x}$$

$$\mathtt{x} \rhd \mathtt{a} = \mathbf{map}\ (+\!\!+ [\mathtt{a}])\ \mathtt{x}$$

Note:

$$(\mathtt{a} \lhd \mathtt{x}) \rhd \mathtt{b} = \mathtt{a} \lhd (\mathtt{x} \rhd \mathtt{b})$$

Define:

$$\mathrm{ldouble}\ \mathtt{x} = 0 \lhd \mathtt{x} +\!\!+ 1 \lhd \mathtt{x}$$

$$\mathrm{rdouble}\ \mathtt{x} = \mathtt{x} \rhd 0\ \curlyvee\ \mathtt{x} \rhd 1$$

Lemma:

$$\mathrm{ldouble} \cdot \mathrm{rdouble} = \mathrm{rdouble} \cdot \mathrm{ldouble}$$

Proof of lemma

$$
\begin{aligned}
& \mathrm{ldouble}\ (\mathrm{rdouble}\ \mathrm{x}) \\
= \quad & \{\ \text{definition of ldouble and rdouble}\ \} \\
& 0 \lhd (\mathrm{x} \rhd 0\ \curlyvee\ \mathrm{x} \rhd 1) \mathbin{+\!\!+} 1 \lhd (\mathrm{x} \rhd 0\ \curlyvee\ \mathrm{x} \rhd 1) \\
= \quad & \{\ \text{naturality of}\ \curlyvee\ \} \\
& (0 \lhd \mathrm{x} \rhd 0\ \curlyvee\ 0 \lhd \mathrm{x} \rhd 1) \mathbin{+\!\!+} (1 \lhd \mathrm{x} \rhd 0\ \curlyvee\ 1 \lhd \mathrm{x} \rhd 1) \\
= \quad & \{\ \text{abide law}\ \} \\
& (0 \lhd \mathrm{x} \rhd 0 \mathbin{+\!\!+} 1 \lhd \mathrm{x} \rhd 0)\ \curlyvee\ (0 \lhd \mathrm{x} \rhd 1 \mathbin{+\!\!+} 1 \lhd \mathrm{x} \rhd 1) \\
= \quad & \{\ \text{naturality of}\ \mathbin{+\!\!+}\ \} \\
& (0 \lhd \mathrm{x} \mathbin{+\!\!+} 1 \lhd \mathrm{x}) \rhd 0\ \curlyvee\ (0 \lhd \mathrm{x} \mathbin{+\!\!+} 1 \lhd \mathrm{x}) \rhd 1 \\
= \quad & \{\ \text{definition of ldouble and rdouble}\ \} \\
& \mathrm{rdouble}\ (\mathrm{ldouble}\ \mathrm{x})
\end{aligned}
$$

Abide law

If x_1 and x_2 are of the same length, then

$$(x_1 \mathbin{+\!\!+} y_1) \mathbin{\curlyvee} (x_2 \mathbin{+\!\!+} y_2) = (x_1 \mathbin{\curlyvee} x_2) \mathbin{+\!\!+} (y_1 \mathbin{\curlyvee} y_2)$$

$$\begin{array}{ccc} x_1 & +\!\!+ & y_1 \\ & \curlyvee & \\ x_2 & +\!\!+ & y_2 \end{array} = \begin{array}{ccc} x_1 & & y_1 \\ \curlyvee & +\!\!+ & \curlyvee \\ x_2 & & y_2 \end{array}$$

Theorem

Define:

$$\text{lbits} = \text{Cons}\ [[]]\ (\text{map ldouble lbits})$$

$$\text{rbits} = \text{Cons}\ [[]]\ (\text{map rdouble rbits})$$

Theorem:

$$\text{lbits} = \text{rbits}$$

Proof of theorem

$$
\begin{aligned}
& \text{lbits} \\
= \quad & \{\ \text{definition of lbits}\ \} \\
& \text{Cons}\ [[]]\ (\text{map ldouble lbits}) \\
= \quad & \{\ \text{proof obligation}\ \} \\
& \text{Cons}\ [[]]\ (\text{map rdouble lbits})
\end{aligned}
$$

Discharging the proof obligation

$$
\begin{array}{ll}
 & \texttt{map rdouble lbits} \\
= & \quad \{\ \text{definition of lbits and rdouble}\ \} \\
 & \texttt{Cons [[0],[1]] (map rdouble (map ldouble lbits))} \\
= & \quad \{\ \text{Lemma}\ \} \\
 & \texttt{Cons [[0],[1]] (map ldouble (map rdouble lbits))} \\
\subset & \quad \{\ \texttt{x} = \texttt{Cons [[0],[1]] (map ldouble x)}\ \text{has a unique solution}\ \} \\
 & \texttt{Cons [[0],[1]] (map ldouble (map ldouble lbits))} \\
= & \quad \{\ \text{definition of lbits and ldouble}\ \} \\
 & \texttt{map ldouble lbits}
\end{array}
$$

Appendix: Streams

$$\text{iterate} :: (a \to a) \to (a \to \text{Stream } a)$$
$$\text{iterate } f\ x = \text{Cons } x\ (\text{iterate } f\ (f\ x))$$

Fusion law:

$$\mathrm{map}\ h \cdot \mathrm{iterate}\ f_1 = \mathrm{iterate}\ f_2 \cdot h \quad \Longleftarrow \quad h \cdot f_1 = f_2 \cdot h$$

$$\begin{array}{ll} & \mathrm{iterate}\ f\ x \\ = & \quad \{\ \text{definition of iterate}\ \} \\ & \mathrm{Cons}\ x\ (\mathrm{iterate}\ f\ (f\ x)) \\ = & \quad \{\ \text{fusion law: } h := f_1 := f_2 := f\ \} \\ & \mathrm{Cons}\ x\ (f\ (\mathrm{iterate}\ f\ x)) \end{array}$$

Appendix: Infinite trees

```
branch :: (a → a) → (a → a) → (a → Tree a)
branch f g x = Node x (branch f g (f x)) (branch f g (g x))
```

Appendix: Proof of abide law

$$P(x_1, x_2) \quad :\Longleftrightarrow \quad (x_1 + y_1) \curlyvee (x_2 + y_2) = (x_1 \curlyvee x_2) + (y_1 \curlyvee y_2)$$

$P([],[])$:

$$
\begin{aligned}
& ([] +\!\!+ y_1) \curlyvee ([] +\!\!+ y_2) \\
= & \quad \{ \text{definition of } +\!\!+ \} \\
& y_1 \curlyvee y_2 \\
= & \quad \{ \text{definition of } \curlyvee \text{ and } +\!\!+ \} \\
& ([] \curlyvee []) +\!\!+ (y_1 \curlyvee y_2)
\end{aligned}
$$

$P(a_1 : x_1, a_2 : x_2)$:

$$
\begin{aligned}
& ((a_1 : x_1) \# y_1) \curlyvee ((a_2 : x_2) \# y_2) \\
= & \quad \{ \text{ definition of } \# \text{ and } \curlyvee \ \} \\
& a_1 : a_2 : ((x_1 \# y_1) \curlyvee (x_2 \# y_2)) \\
= & \quad \{ \text{ ex hypothesi } \} \\
& a_1 : a_2 : ((x_1 \curlyvee x_2) \# (y_1 \curlyvee y_2)) \\
= & \quad \{ \text{ definition of } \# \ \} \\
& (a_1 : a_2 : (x_1 \curlyvee x_2)) \# (y_1 \curlyvee y_2) \\
= & \quad \{ \text{ definition of } \curlyvee \ \} \\
& ((a_1 : x_1) \curlyvee (a_2 : x_2)) \# (y_1 \curlyvee y_2)
\end{aligned}
$$