

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

```
data Stream a = Cons a (Stream a)
```

```
nat = Cons 0 (map (+1) nat)
```

```
nat = iterate (+1) 0
```

Background: Infinite trees

```
data Tree a = Node (Tree a) a (Tree a)
```

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

```
nat = branch ( $\lambda i \rightarrow 2 * i + 1$ ) ( $\lambda i \rightarrow 2 * i + 2$ ) 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:

$$a \triangleleft x = \text{map } ([a] \#) x$$

$$x \triangleright a = \text{map } (\# [a]) x$$

Note:

$$(a \triangleleft x) \triangleright b = a \triangleleft (x \triangleright b)$$

Define:

$$\text{ldouble } x = 0 \triangleleft x \# 1 \triangleleft x$$

$$\text{rdouble } x = x \triangleright 0 \vee x \triangleright 1$$

Lemma:

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

Proof of lemma

$$\begin{aligned} & \text{ldouble (rdouble x)} \\ = & \quad \{ \text{definition of ldouble and rdouble} \} \\ & 0 \triangleleft (x \triangleright 0 \vee x \triangleright 1) \# 1 \triangleleft (x \triangleright 0 \vee x \triangleright 1) \\ = & \quad \{ \text{naturality of } \vee \} \\ & (0 \triangleleft x \triangleright 0 \vee 0 \triangleleft x \triangleright 1) \# (1 \triangleleft x \triangleright 0 \vee 1 \triangleleft x \triangleright 1) \\ = & \quad \{ \text{abide law} \} \\ & (0 \triangleleft x \triangleright 0 \# 1 \triangleleft x \triangleright 0) \vee (0 \triangleleft x \triangleright 1 \# 1 \triangleleft x \triangleright 1) \\ = & \quad \{ \text{naturality of } \# \} \\ & (0 \triangleleft x \# 1 \triangleleft x) \triangleright 0 \vee (0 \triangleleft x \# 1 \triangleleft x) \triangleright 1 \\ = & \quad \{ \text{definition of ldouble and rdouble} \} \\ & \text{rdouble (ldouble x)} \end{aligned}$$

Abide law

If x_1 and x_2 are of the same length, then

$$(x_1 \# y_1) \vee (x_2 \# y_2) = (x_1 \vee x_2) \# (y_1 \vee y_2)$$

$$\begin{array}{ccccc} x_1 & \# & y_1 & & x_1 & & y_1 \\ & & \vee & = & \vee & \# & \vee \\ x_2 & \# & y_2 & & x_2 & & y_2 \end{array}$$

Theorem

Define:

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

Theorem:

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

Proof of theorem

lbits
= { definition of lbits }
Cons [[]] (map ldouble lbits)
= { proof obligation }
Cons [[]] (map rdouble lbits)

Discharging the proof obligation

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

Appendix: Streams

```
iterate :: (a -> a) -> (a -> Stream a)
iterate f x = Cons x (iterate f (f x))
```

Fusion law:

$$\text{map } h \cdot \text{iterate } f_1 = \text{iterate } f_2 \cdot h \quad \Leftarrow \quad h \cdot f_1 = f_2 \cdot h$$

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

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

$$P(\mathbf{x}_1, \mathbf{x}_2) \quad :\iff \quad (\mathbf{x}_1 \# \mathbf{y}_1) \vee (\mathbf{x}_2 \# \mathbf{y}_2) = (\mathbf{x}_1 \vee \mathbf{x}_2) \# (\mathbf{y}_1 \vee \mathbf{y}_2)$$

$P([], [])$:

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

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

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