Solution For Assignment 2

Bogdan Dumitriu

September 17, 2004

Exercise 1

PROOF asgn2_1

[D1:] $\texttt{sumsum1 ss} = \texttt{SUM (map SUM ss)}$
[D2:] $\texttt{sumsum2 ss} = \texttt{foldr (s r} \rightarrow \texttt{SUM s} + \texttt{r) 0 ss}$
[G1:] $(\forall \texttt{ss} :: \texttt{sumsum1 ss} = \texttt{sumsum2 ss})$

BEGIN

1 {See proof Pbase}

sumsum1 [] = sumsum2 []

EQUATIONAL PROOF Pbase

sumsum1 []

= {By definition of sumsum1 (D1)}

SUM (map SUM [])

= {By definition of map}

SUM []

= {By definition of SUM}

0

= {By definition of foldr}

foldr (s r → SUM s + r) 0 []

= {By definition of sumsum2 (D2)}

sumsum2 []

END

2 {See proof Pinduct}

$(\forall \texttt{x}, \texttt{s} :: (\texttt{sumsum1 s} = \texttt{sumsum2 s}) \Rightarrow (\texttt{sumsum1 (x : s)} = \texttt{sumsum2 (x : s)}))$

PROOF Pinduct

[A1:] [ANY x, s] sumsum1 s = sumsum2 s

[G1:] sumsum1 (x : s) = sumsum2 (x : s)

BEGIN

1 {See proof eqq}

sumsum1 (x : s) = sumsum2 (x : s)

EQUATIONAL PROOF eqq

```
sumsum2 (x : s)
= {By definition of sumsum2 (D2)}
foldr (s r → SUM s + r) 0 (x : s)
= {By definition of foldr}
SUM x + (foldr (s r → SUM s + r) 0 s)
= {By definition of sumsum2 (D2)}
SUM x + (sumsum2 s)
= {A1}
SUM x + (sumsum1 s)
= {By definition of sumsum1 (D1)}
SUM x + (SUM (map SUM s))
= {By definition of SUM}
SUM ((SUM x) : (map SUM s))
= {By definition of map}
SUM (map SUM (x : s))
= {By definition of sumsum1 (D1)}
sumsum1 (x : s)
```

END ____

END ____

3 {List induction on 1 and 2}
(∀s :: sumsum1 s = sumsum2 s)

4 {Rename bound variable of 3}
(∀ss :: sumsum1 ss = sumsum2 ss)

END ____

Exercise 2

Note 1: The problem, as described in the text of the assignment, is somewhat ambiguous in saying whether or not additional blue candies (i.e. blue candies which are not initially in the box) can be used when taking out a white candy. The program specification, however, implies that additional candies can (and will, if needed) be used when wanting to take out a white candy without having at least two _original_ blue candies available out of the box in order to put them back in. This is justified by the fact that $w > 0$ is the only condition for taking out a white candy (i.e. there is no additional condition specifying that at least two of the _original_ blue candies have to be outside of the box in order for a white candy to be taken out). The following proof is thus based on the program specification itself, which allows the use of additional blue candies.

Note 2: I have added a new instruction to the program, just before $n := 0$, in order to store the value of the expression $3 * w + b$ computed using the initial values of w and b into the local variable WB. As this is just an assignment to a local variable, it does not interfere with the program in any way. I have introduced this extra variable because there was no other way in which I could specify the termination metric and then be still able to prove everything that needs to be proven.

The proof plan:

```
CANDY(OUT b, w, n : int)

int WB; {See note 2}

{* b ≥ 1 ∧ w ≥ 1, see PROOF Init *}

WB := 3 * w + b; {See note 2}
n := 0;

{* I, see PROOFs PTC1a, PTC1b, PTC2, PEC, PICa, PICb.
      Termination metric : WB − n *}

while
    b > 0 do { b := b − 1; n := n + 1 }
    w > 0 do { w := w − 1; b := b + 2; n := n + 1 }

{* (b = 0) ∧ (w = 0) ∧ n ≥ 3 *}

ASSUMING

I = (WB − n = 3 * w + b) ∧ (b ≥ 0) ∧ (w ≥ 0) ∧ (WB ≥ 4)
```

The proof(s):

PROOF Init

[A1:] $b \geq 1 \wedge w \geq 1$
[D1:] $Q = wp\ (WB := 3 * w + b;\ n := 0)\ I$
[G1:] Q

BEGIN ____

1 {Rewrite D1 with definition of I and definition of wp}
$Q = (3 * w + b - 0 = 3 * w + b) \wedge (b \geq 0) \wedge (w \geq 0) \wedge (3 * w + b \geq 4)$

2 {Trivial}
$3 * w + b - 0 = 3 * w + b$

3 {∧-Elimination on A1}
$b \geq 1$

4 {∧-Elimination on A1}
$w \geq 1$

5 {Trivial, from 3}
$b \geq 0$

6 {Trivial, from 4}
$w \geq 0$

7 {Trivial, from 3 and 4}
$3 * w + b \geq 4$

8 {Conjunction of 2, 5, 6 and 7}

$(3 * w + b - 0 = 3 * w + b) \land (b \geq 0) \land (w \geq 0) \land (3 * w + b \geq 4)$

9 {Rewrite 8 with 1}

Q

END

PROOF PTC1a

[A1:] I
[A2:] $b > 0$
[D1:] $Q = wp\ (C := WB - n;\ b := b - 1;\ n := n + 1)\ (WB - n < C)$
[G1:] Q

BEGIN

1 {Rewrite D1 with definition of wp}

$Q = WB - (n + 1) < WB - n$

2 {Trivial, from 1}

$Q = -1 < 0$

3 {Trivial}

$-1 < 0$

4 {Rewrite 3 with 2}

Q

END

PROOF PTC1b

[A1:] I
[A2:] $w > 0$
[D1:] $Q = wp\ (C := WB - n;\ w := w - 1;\ b := b + 2;\ n := n + 1)\ (WB - n < C)$
[G1:] Q

BEGIN

1 {Rewrite D1 with definition of wp}

$Q = WB - (n + 1) < WB - n$

2 {Trivial, from 1}

$Q = -1 < 0$

3 {Trivial}

$-1 < 0$

4 {Rewrite 3 with 2}

Q

END

PROOF PTC2

[A1:] $\mathtt{I}$
[A2:] $\mathtt{b} > 0 \vee \mathtt{w} > 0$
[G1:] $\mathtt{WB} - \mathtt{n} > 0$

BEGIN

1 {Rewrite A1 with definition of I}
$(\mathtt{WB} - \mathtt{n} = 3 * \mathtt{w} + \mathtt{b}) \wedge (\mathtt{b} \geq 0) \wedge (\mathtt{w} \geq 0) \wedge (\mathtt{WB} \geq 4)$

2 {$\wedge$-Elimination on 1}
$\mathtt{WB} - \mathtt{n} = 3 * \mathtt{w} + \mathtt{b}$

3 {$\wedge$-Elimination on 1}
$\mathtt{b} \geq 0$

4 {$\wedge$-Elimination on 1}
$\mathtt{w} \geq 0$

5 {Trivial, justified by 4}
$\mathtt{b} > 0 \Rightarrow 3 * \mathtt{w} + \mathtt{b} > 0$

6 {Trivial, justified by 3}
$\mathtt{w} > 0 \Rightarrow 3 * \mathtt{w} + \mathtt{b} > 0$

7 {Case split on A2, 5 and 6}
$3 * \mathtt{w} + \mathtt{b} > 0$

8 {Rewrite 7 with 2}
$\mathtt{WB} - \mathtt{n} > 0$

END

PROOF PEC

[A1:] $\mathtt{I}$
[A2:] $\neg(\mathtt{b} > 0)$
[A3:] $\neg(\mathtt{w} > 0)$
[G1:] $(\mathtt{b} = 0) \wedge (\mathtt{w} = 0) \wedge \mathtt{n} \geq 3$

BEGIN

1 {Rewrite A1 with definition of I}
$(\mathtt{WB} - \mathtt{n} = 3 * \mathtt{w} + \mathtt{b}) \wedge (\mathtt{b} \geq 0) \wedge (\mathtt{w} \geq 0) \wedge (\mathtt{WB} \geq 4)$

2 {$\wedge$-Elimination on 1}
$\mathtt{WB} - \mathtt{n} = 3 * \mathtt{w} + \mathtt{b}$

3 {$\wedge$-Elimination on 1}
$\mathtt{b} \geq 0$

4 {∧-Elimination on 1}

$w \geq 0$

5 {Trivial, from A2 and 3}

$b = 0$

6 {Trivial, from A3 and 4}

$w = 0$

7 {Rewrite 2 with 5 and 6}

$WB - n = 3 * 0 + 0$

8 {Trivial, from 7}

$n = WB$

9 {∧-Elimination on 1}

$WB \geq 4$

10 {Rewrite 9 with 8}

$n \geq 4$

11 {Trivial, from 10}

$n \geq 3$

12 {Conjunction of 5, 6 and 11}

$(b = 0) \wedge (w = 0) \wedge n \geq 3$

END

PROOF PICa

[A1:] I
[A2:] $b > 0$
[D1:] $Q = wp\ (b := b - 1;\ n := n + 1)\ I$
[G1:] Q

BEGIN

1 {Rewrite D1 with definition of I}

$Q = wp\ (b := b{-}1;\ n := n{+}1)\ ((WB{-}n = 3{*}w{+}b){\wedge}(b \geq 0){\wedge}(w \geq 0){\wedge}(WB \geq 4))$

2 {Rewrite 1 with definition of wp}

$Q = (WB - n - 1 = 3 * w + b - 1) \wedge (b - 1 \geq 0) \wedge (w \geq 0) \wedge (WB \geq 4)$

3 {Rewrite A1 with definition of I}

$(WB - n = 3 * w + b) \wedge (b \geq 0) \wedge (w \geq 0) \wedge (WB \geq 4)$

4 {∧-Elimination on 3}

$WB - n = 3 * w + b$

5 {Trivial, from 4}

$WB - n - 1 = 3 * w + b - 1$

6 {∧-Elimination on 3}

$w \geq 0$

7 {Trivial, from A2}

$b - 1 \geq 0$

8 {∧-Elimination on 3}

$WB \geq 4$

9 {Conjunction on 5, 7, 6 and 8}

$(WB - n - 1 = 3 * w + b - 1) \wedge (b - 1 \geq 0) \wedge (w \geq 0) \wedge (WB \geq 4)$

10 {Rewrite 9 with 2}

Q

END

PROOF PICb

[A1:] I
[A2:] $w > 0$
[D1:] $Q = wp\ (w := w - 1;\ b := b + 2;\ n := n + 1)\ I$
[G1:] Q

BEGIN

---

1 {Rewrite D1 with definition of I}

$Q = wp\ (w := w{-}1;\ b := b{+}2;\ n := n{+}1)\ ((WB{-}n = 3{*}w{+}b) \wedge (b \geq 0) \wedge (w \geq 0) \wedge (WB \geq 4)))$

2 {Rewrite 1 with definition of wp}

$Q = (WB - n - 1 = 3 * w - 3 + b + 2) \wedge (b + 2 \geq 0) \wedge (w - 1 \geq 0) \wedge (WB \geq 4)$

3 {Rewrite A1 with definition of I}

$(WB - n = 3 * w + b) \wedge (b \geq 0) \wedge (w \geq 0) \wedge (WB \geq 4)$

4 {∧-Elimination on 3}

$WB - n = 3 * w + b$

5 {Trivial, from 4}

$WB - n - 1 = 3 * w - 3 + b + 2$

6 {∧-Elimination on 3}

$b \geq 0$

7 {Trivial, from 6}

$b + 2 \geq 0$

8 {Trivial, from A2}

$w - 1 \geq 0$

9 {∧-Elimination on 3}

$WB \geq 4$

10 {Conjunction on 5, 7, 8 and 9}

$(\mathtt{WB} - \mathtt{n} - 1 = 3 * \mathtt{w} - 3 + \mathtt{b} + 2) \wedge (\mathtt{b} + 2 \geq 0) \wedge (\mathtt{w} - 1 \geq 0) \wedge (\mathtt{WB} \geq 4)$

11 {Rewrite 10 with 2}

Q

END