CMU 17-651 Models of Software Systems Fall 2018

Homework #4:

Structures, Equational Reasoning, and Induction

Dario A Lencina-Talarico Due: 24 September 2018

I. Sets, Relations, and Functions

1. Use set comprehension to define the set $SumOfSquares$ containing all the natural numbers that can be expressed as the sum $a^2 + b^2$ where a and b are natural numbers.
   $\mathit{SumOfSquares} == \{x : \mathbb{N} \mid (\exists\, a : \mathbb{N})(\exists\, b : \mathbb{N}) \bullet x = a^2 + b^2\}$

2. Write out in full the powersets of each of the following.
   a. $\mathbb{P}\{7, 1\} = \{\emptyset, \{1\}, \{7\}, \{7, 1\}\}$
   b. $\mathbb{P}\{5\} = \{\emptyset, \{5\}\}$
   c. $\mathbb{P}\emptyset = \{\emptyset\}$
   d. $\mathbb{P}\{\emptyset\} = \{\emptyset, \{\emptyset\}\}$

3. Write out in full the following Cartesian products.
   a. $\{4, 2\} \times \{2, 4\} = \{(4, 2), (4, 4), (2, 2), (2, 4)\}$
   b. $\{0\} \times \emptyset = \emptyset$
   c. $\{1, 2\} \times \{a\} = \{(1, a), (2, a)\}$
   d. $\{\emptyset\} \times \{a\} = \{\emptyset\}$

4. Suppose $R == 2 \mathrel{..} 5$ and $S == 4 \mathrel{..} 6$. Enumerate the elements of the following sets.
   a. $R \cup S = \{2, 3, 4, 5, 6\}$
   b. $R \cap S = \{4, 5\}$
   c. $R \setminus S = \{2, 3\}$
   d. $S \setminus R = \{6\}$
   e. $S \times R = \{(4, 2), (4, 3), (4, 4), (4, 5), (5, 2), (5, 3), (5, 4), (5, 5), (6, 2), (6, 3), (6, 4), (6, 5)\}$

5. Let S be the set of numbers from 1 to 12 inclusive. Let R be a relation, such that $R : S \leftrightarrow S$ and such that x is related to y exactly when y is greater than the square of x but less than the square of $x + 1$. Provide an axiomatic definition for R.
   (Note: be sure to check your notation and formatting — refer to page 152 in GWC10.)

6. Suppose Let and Num are defined as follows:

$$\begin{aligned} \mathit{Let} &== \{a, b, c, d, e\} \\ \mathit{Num} &== \{1, 2, 3, 4, 5\} \end{aligned}$$

   a. Give an example of each of the following:
      i. A function whose declaration is $Let \to Num$
         $f1 == \{a \mapsto 1, b \mapsto 2, c \mapsto 3, d \mapsto 4, e \mapsto 5\}$

ii. A function whose declaration is $Let \pfun Num$
$f2 == \{a \mapsto 1, b \mapsto 2, c \mapsto 3\}$

iii. A total injection from Let to Num
$f3 == \{a \mapsto 1, b \mapsto 2, c \mapsto 3, d \mapsto 4, e \mapsto 5\}$

b. Is it possible to give an example of a total injection from Let to $\{1, 2, 3, 4\}$? If so, provide one; if not, explain why not.
No because the number of values in the source is larger that the target and we can not map more than one source element to the same target because that will violate the injection rule.

II. Proof: Equational Reasoning

You may use any of the following theorems in your equational proofs:

$\vdash p \wedge true \;\Leftrightarrow\; p$	$\wedge$-True
$\vdash p \wedge false \;\Leftrightarrow\; false$	$\wedge$-False
$\vdash p \vee true \;\Leftrightarrow\; true$	$\vee$-True
$\vdash p \vee false \;\Leftrightarrow\; p$	$\vee$-False
$\vdash p \vee \neg p$	Excluded Middle
$\vdash p \vee q \;\Leftrightarrow\; q \vee p$	$\vee$-Commutativity
$\vdash p \wedge q \;\Leftrightarrow\; q \wedge p$	$\wedge$-Commutativity
$\vdash (p \vee q) \vee r \;\Leftrightarrow\; p \vee (q \vee r)$	$\vee$-Associativity
$\vdash (p \wedge q) \wedge r \;\Leftrightarrow\; p \wedge (q \wedge r)$	$\wedge$-Associativity
$\vdash p \vee (q \wedge r) \;\Leftrightarrow\; (p \vee q) \wedge (p \vee r)$	$\vee\wedge$-Distributivity
$\vdash p \wedge (q \vee r) \;\Leftrightarrow\; (p \wedge q) \vee (p \wedge r)$	$\wedge\vee$-Distributivity
$\vdash p \Rightarrow q \;\Leftrightarrow\; \neg p \vee q$	$\Rightarrow$-Alternative
$\vdash p \Rightarrow q \;\Leftrightarrow\; \neg q \Rightarrow \neg p$	Contrapositives
$\vdash \neg\neg p \;\Leftrightarrow\; p$	Double Negation
$\vdash \neg(p \wedge q) \;\Leftrightarrow\; \neg p \vee \neg q$	De Morgan
$\vdash \neg(p \vee q) \;\Leftrightarrow\; \neg p \wedge \neg q$	De Morgan
$\vdash x \in \emptyset \;\Leftrightarrow\; false$	$\emptyset$ Membership

7. Prove in equational style the following laws for set union:

   a. $S \cup T = T \cup S$
      $\Leftrightarrow$ [Definition of $\cup$]
      $x \in S \vee x \in T$
      $\Leftrightarrow$ [$\vee$ commutative]
      $x \in T \vee x \in S$
      Hence, $x \in S \vee x \in T \Leftrightarrow x \in T \vee x \in S$
      Since x was arbitrary, we have $\exists - Intro$
      $\exists\, x : T \bullet (x \in S \vee x \in T \Leftrightarrow x \in T \vee x \in S)$
      By the definition of set equality
      $S \cup T = T \cup S$ QED

   b. $S \cap \emptyset = \emptyset$
      $\Leftrightarrow$ [Definition of $\cup$]
      $x \in S \wedge x \in \emptyset$
      $\Leftrightarrow$ [*emptyset* Membership]
      $x \in T \wedge false$
      $\Leftrightarrow$ [Applying $\wedge$ *truthtables*]
      $false = \emptyset$ QED

   (HINT: To prove $S = T$ show $\forall\, x : U \bullet x \in S \Leftrightarrow x \in T$, where U is the type of elements in sets S and T.)

8. Prove the following theorem in equational style:

$$\vdash \neg(\neg p \Rightarrow (q \wedge r)) \;\Leftrightarrow\; (\neg p \wedge \neg q) \vee (\neg p \wedge \neg r)$$

III. Sequences

9. Define the following sequences by enumeration:

a. *Threes*: natural numbers smaller than 18 that are divisible by 3.
Using GWC10 notation for seq enums definition:
$Threes ::= 3 \mid 6 \mid 9 \mid 12 \mid 15$

b. *Twos*: natural numbers smaller than 20 that are divisible by 2.
Using GWC10 notation for seq enums definition:
: $Twos ::= 2 \mid 4 \mid 6 \mid 8 \mid 10 \mid 12 \mid 14 \mid 16 \mid 18$

10. Given the above, what are each of the following:

a. $Threes \cup Twos$
$Threes \cup Twos == < 2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18 >$

b. $Threes \cap Twos$
Empty sequence: $<>$

c. dom *Threes*

d. ran *Threes*

e. $\mathrm{dom}\ Twos \lhd Threes$

f. $(5 \mathrel{..} 8) \lhd (Threes \frown Twos)$
(NOTE: $\frown$ is the concatenation operator).

IV. Proof: Natural Induction

Prove the following claim by induction over the natural numbers:

$$0^2 + 1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$$

V. Proof: Structural Induction

Consider the definition of binary trees in Chapter 7.

(a) Show that

$$\forall\, t : TREE \bullet leaves(t) = nodes(t) + 1$$

(b) Define a *mirror* function that recursively swaps the branches of a tree.

(c) Using the definition of *mirror* show that

$$\forall\, t : TREE \bullet size(mirror(t)) = size(t)$$

(d) Using the definition of *mirror* show that

$$\forall\, t : TREE \bullet mirror(mirror(t)) = t$$

(HINT: use structural induction over trees.)