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.
   Redo note: Adjusted parenthesis
   $\mathit{SumOfSquares} == \{x : \mathbb{N} \mid \exists\, a : \mathbb{N} \bullet \exists\, b : \mathbb{N} \bullet x = a^2 + b^2\}$

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. $\{\emptyset\} \times \{a\} = \{(\emptyset, a)\}$
   Redo note: Defined pair

4. Suppose $R == 2 \,..\, 5$ and $S == 4 \,..\, 6$. 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.)
   Redo note: Added equation
   $S == \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

$$R : S \rightarrow S$$

$$\forall\, x, y : S \bullet (x, y) \in S \Leftrightarrow (x^2 < y) \wedge (y < (x + 1)^2)$$

6. Suppose Let and Num are defined as follows:

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

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 $Let \nrightarrow Num$
   $f2 == \{a \mapsto 1, b \mapsto 2, c \mapsto 3\}$

   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. $S \cup T = T \cup S$

   Redo note: Adjusted proof

   $x \in S \cup T$
   $\Leftrightarrow$ [Definition of $\cup$]
   $x \in S \vee x \in T$
   $\Leftrightarrow$ [$\vee$ commutative]
   $x \in T \vee x \in S$
   $\Leftrightarrow$ [Definition of $\cup$]
   $x \in T \cup S$
   $S \cup T = T \cup S$ QED

   b. $S \cap \emptyset = \emptyset$

   Redo note: Adjusted proof

   $x \in S \cap \emptyset$
   $\Leftrightarrow$ [Definition of $\cap$]
   $x \in S \wedge x \in \emptyset$
   $\Leftrightarrow$ [*emptyset* Membership]
   $x \in T \wedge false$
   $\Leftrightarrow$ [arithmetic]
   $\emptyset$
   $S \cap \emptyset = \emptyset$ 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:

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

Redo note: Added proof

$\neg(\neg p \Rightarrow (q \wedge r))$
$\Leftrightarrow$ [$\Rightarrow$-Alternative]
$\neg(p \vee (q \wedge r))$
$\Leftrightarrow$ [$\vee\wedge$ - Distributibity]
$\neg((p \vee q) \wedge (p \vee r))$
$\Leftrightarrow$ [De Morgan]
$(\neg p \wedge \neg q) \vee (\neg p \wedge \neg r)$

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:
   $Threes == < 3, 6, 9, 12, 15 >$

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

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

    a. $Threes \cup Twos$
    Redo note: Transformed to sets and applied $\cup$.
    $TreesAsSetOfPairs = \{(1,3),(2,6),(3,9),(4,12),(5,15)\}$
    $TwosAsSetOfPairs = \{(1,2),(2,4),(3,6),(4,8),(5,10),(6,12),(7,14),(8,16),(9,18)\}$
    $Threes \cup Twos = \{(1,3),(2,6),(3,9),(4,12),(5,15),(1,2),(2,4),(3,6),(4,8),(5,10),(6,12),(7,14),(8,16),(9,18)\}$

    b. $Threes \cap Twos$
    Redo note: Transformed to sets and applied $\cap$.
    $Threes \cap Twos = \{\emptyset\}$

    c. $\mathrm{dom}\ Threes == \{1, 2, 3, 4, 5\}$
    To get the domain of a sequence, we just need to get the indexes from 1 up to the cardinality of the sequence.

    d. $\mathrm{ran}\ Threes == \{3, 6, 9, 12, 15\}$

    e. $\mathrm{dom}\ Twos \lhd Threes$
    $\lhd$ is the domain restrictor operator, informally, the restricted relation contains those elements from Three whose first component appears in Two.
    $domTwos == \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
    Redo note: Corrected set notation.
    $\mathrm{dom}\ Twos \lhd Threes == < 3, 6, 9, 12, 15 >$

    f. $(5 \mathinner{..} 8) \lhd (Threes \frown Twos)$
    $Threes \frown Twos == < 3, 6, 9, 12, 15, 2, 4, 6, 8, 10, 12, 14, 16, 18 >$
    $\lhd$ is asking us to filter elements from 5 ..8
    Redo note: Corrected notation to set and swaped 5 to 6.
    $(5 \mathinner{..} 8) \lhd (Threes \frown Twos) == \{15, 2, 4, 6\}$ (NOTE: $\frown$ is the concatenation operator).

IV. Proof: Natural Induction

Prove the following claim by induction over the natural numbers:

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

Base case:
$P(0) = \frac{0}{6} = 0$
$0^2 = 0$
Inductive step We assume that $k \in \mathbb{N}$ and P(k) holds. We then show that P(k+1) holds, that is $0^2 + 1^2 + 2^2 + ... + k + (k+1)^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6} = \frac{2k^3+9k^2+13K+6}{6}$
$0^2 + 1^2 + 2^2 + ... + k + (k+1)^2$
$=$ [substitution, induction hypothesis]
$\frac{k(k+1)(2k+1)}{6} + (k+1)^2$
$=$ [arithmetic]
$\frac{(k^2+k)(2k+1)}{6} + (k+1)^2$
$=$ [arithmetic]
$\frac{2k^3+9k^2+13K+6}{6}$

V. Proof: Structural Induction

Consider the definition of binary trees in Chapter 7.

(a) Show that

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

Redo Note: Added proof:
$\mathit{size} : \mathit{TREE} \rightarrow \mathbb{N}$

$\forall\, t1, t2 : \mathit{TREE} \bullet$
$\mathit{size}(\mathit{leaf}) = 1 \land$
$\mathit{size}(\mathit{node}(t1, t2) = 1 + \mathit{size}(t1) + \mathit{size}(t2)$

$\mathit{leaves} : \mathit{TREE} \rightarrow \mathbb{N}$
$\mathit{nodes} : \mathit{TREE} \rightarrow \mathbb{N}$

$\forall\, t1, t2 : \mathit{TREE} \bullet$
$\mathit{leaves}(\mathit{leaf}) = 1 \land$
$\mathit{leaves}(\mathit{node}(t1, t2)) = \mathit{leaves}(t1) + \mathit{leaves}(t2) \land$
$\mathit{nodes}(\mathit{leaf}) = 0 \land$
$\mathit{nodes}(\mathit{node}(t1, t2)) = 1 + \mathit{nodes}(t1) + \mathit{nodes}(t2)$

Base Case: Show the property holds for leaf, that is, leaves(leaf) = 1
$\mathit{leaves}(\mathit{leaf})$
$=$ [definition of leaves]
0 + 1
$=$ [definiton of nodes]
nodes(leaf) + 1

Induction case: Generalize base case for leaves(t1) = nodes(t1) + 1 and leaves(t2) = nodes(t2) + 1

leaves(node(t1,t2))	
=	[applying definiton of leaves]
leaves(t1) + leaves(t2)	
=	[induction hypotesis]
nodes(t1) + 1 + nodes(t2) + 1	
=	[transforming the nodes back to leaves using nodes(node(t1,t2))]
nodes(t) + 1	

(b) Define a *mirror* function that recursively swaps the branches of a tree.
The idea of this function is that it recursively calls mirror swapping t1 and t2 every time that it finds a node. If it finds a leaf it just returns.

$mirror : TREE \to TREE$

Redo note: fixed equation, the key aspect is changing the order of t1, t2 and calling $mirror(node)$ recursively.
$\forall\, t1, t2 : TREE \bullet$
$mirror(leaf) = leaf \land$
$mirror(node(t1, t2)) = node(mirror(t2), mirror(t1))$

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

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

Using the definition of size(t) provided in GWC10:

$size : TREE \to \mathbb{N}$

$\forall\, t1, t2 : TREE \bullet$
$size(leaf) = 1 \land$
$size(node(t1, t2) = 1 + size(t1) + size(t2)$

Proof:
Base Case: Show the property holds for leaf, that is, size(leaf) = size(mirror(leaf))
Redo note: Corrected equation for mirror(node).

size(leaf)	
=	[definition size(mirror(leaf))]
size(mirror(leaf))	
=	[since mirror(leaf) = leaf] size(leaf)
1	

Redo note: Corrected induction hypotesis.
Induction case: Assume that the property holds for trees t1 and t2, that is size(mirror(t1)) = size(t1), and size(mirror(t2)) = size(t2). Show that it holds for node(t1,t2)

size(mirror(node(t1,t2)))
= [definition of mirror(node)]
size(node(mirror(t2), mirror(t1)))
= [applying distributive property of size] size(mirror(t2)) + size(mirror(t1)
size(t2) + size(t1)
= [applying distributive property of size]
size(t)

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

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

(HINT: use structural induction over trees.)
Proof:
Base Case: Show the property holds for leaf, that is, leaf = mirror(leaf)

mirror(mirror(leaf))
= [applying definition mirror(leaf)]
mirror(leaf)
= [applying definition of mirror(leaf)
leaf QED

Induction case: Assume that the property holds for trees t1 and t2, that is mirror(mirror(node(t1,t2))) = node(t1,t2)

mirror(mirror(node(t1,t2)))
= [definition of mirror]
mirror(node(mirror(t2), mirror(t1)))
= [applying mirror function again]
node(node(t1',t2'), node(node(t2',t1'))
= [if t1 = (node(t1',t2') and t2 = node(t2', t1')]
node(t1, t2) QED