UNIVERSITY BORDEAUX 1
MASTER INFORMATIC - SOFTWARE ENGINEERING

A PROJECT REPORT
ON

FORMAL DESIGN

BY

NGUYEN Quang Anh

2014-2015

ABSTRACT

Formal Methods in System Design allows the designing, implementing, and validating the correctness of the system. In this project, I implemented and proved the correctness of the machines that check a given array if it's sorted in ascending order, sorted (ascending or descending), check two given arrays if they are identicals, if one array included the other, and sort a given array in ascending order

The purpose of this paper, is to deliver the process of proving the proof obligations, those that was proved interactively, as well as the reasoning for the unproved ones.

1 INTRODUCTION

In the last lesson of Formal Design, we were given a project to finish. Our job is to design several machines that :

- check if a given array is sorted in ascending order
- check if a given array is sorted (ascending or descending order)
- check if two given arrays are identical
- given two arrays, check if one array included the other one
- given an array with pairwise distinct values, sort this array in ascending order
- given an array, sort this array in ascending order

I used a software, named **Rodin**, to do this project. Some theories will be proved in this paper, if cannot be proved in the program.

2 Check if array is sorted in ascending order

- Specification: TestAscendingMachine
- Implementation: TestAscendingMachineImplementation

The only PO that need to be proved interactively, is **liveness/WD** int **TestAscendingMachineImplementation**. I proved this using tthe tactic **Disjunction to implication**

3 Check if array is sorted

- Specification: TestSortedMachine
- Implementation: TestSortedMachineImplementation

The POs that need to be proved interactively is :

- inv9/WD
- liveness/WD
- liveness/THM
- INITIALISATION/inv7/INV
- IS_SORTED/grd1/GRD
- LOOP_EQUAL/inv9/INV

The only tatic that I used, is **Disjuction to implication**

4 Check if two given arrays are identical

- Specification: CompareArraysMachine
- Implementation: CompareArraysMachineImplementation

The POs that need to be proved interactively:

- In CompareArraysMachine
  - NOT_IDENTICAL/grd1/WD
- In CompareArraysMachineImplementation
  - liveness/WD
  - IS_IDENTICAL/grd1/GRD
  - NOT_IDENTICAL/grd1/WD

The only tactic used to solve, is **Disjuction to implication**

5 Check if the values of one array is included in another one

- Specification: ValueIncludedMachine
- Implementation:
  - ValueIncludedMachineImplementation
  - ValueIncludedMachineImplementation2

ValueIncludedMachineImplementation is a machine that check the values of the two arrays whether they satisfy :

$$\forall i \cdot i \in dom(array1) \Rightarrow (\exists j \cdot j \in dom(array2) \Rightarrow array1(i) = array2(j))$$

The complexity of this problem is:

$$O(n_1, n_2) = n_1.n_2 \quad n_1 = card(dom(array1)) \land n_2 = card(dom(array2))$$

ValueIncludedMachineImplementation2 is a special case of **ValueIncludedMachineImplementation**, where the two given arrays are sorted in ascending order.

$$O(n_1, n_2) = n_1 + n_2 \quad n_1 = card(dom(array1)) \land n_2 = card(dom(array2))$$

The POs that need to be proved interactively are:

- liveness/WD (in both of the implementations)
- liveness/THM (in both of the implementations)

The tactic that was used to prove, is **Disjunction to implication**

6 Sort an array pairwised distinct values

- Specification: SortArrayDistinctValueMachine
- Implementation: SortArrayDistinctValueAscendingMachineImplementation

In this machine, the POs that need to be proved interactively is many, and the proving process is more complicated than before.

6.1 LOOP_SWAP/inv6/INV

I added some hypotheses:

- $a'(last\_index + 1) = a(last\_index + 1)$
- $last\_index + 1 > indice + 1$
- $i = indice \lor i = indice + 1 \lor (i \neq indice \land i \neq indice + 1)$

6.2 LOOP_SWAP/inv7/INV

Hypothese added:
$i = indice \lor i = indice + 1 \lor i < indice$
After that, I proved by case. First case, $i < indice$, add hypothese : $a'(i) = a(i)$.
For two last cases, $i = indice \lor i = indice + 1$, it was proved automatic.

6.3 LOOP_SWAP/inv10/INV

Demonstrate:

$$\forall\, i \cdot i \in last\_index + 1..size \land i + 1 \in last\_index + 1..size \Rightarrow a'(i) \leq a'(i + 1)$$

I applied this hypothese for i and $i + 1$

$$\forall\, i \cdot i \in 1..size \land \neg i = indice \land \neg i = indice + 1 \Rightarrow a'(i) = a(i)$$

After that I applied this hypothese, and it was done.

$$\forall\, i \cdot i \in \mathit{last\_index} + 1..\mathit{size} \wedge i + 1 \in \mathit{last\_index} + 1..\mathit{size} \Rightarrow a(i) \leq a(i + 1$$

6.4 LOOP_SWAP/inv12/INV

Demonstrate:

$$\forall\, i \cdot i \in 1..\mathit{size} \Rightarrow (\exists\, j \cdot j \in 1..\mathit{size} \Rightarrow \mathit{array}(i) = a'(j))$$

Applying case distinction :

$$i = \mathit{indice} \vee i = \mathit{indice} + 1 \vee (i \neq \mathit{indice} \wedge i \neq \mathit{indice} + 1)$$

After that, each case was proved automatically.

6.5 LOOP_SWAP/act4/FIS

Prove that :

$$\begin{aligned}
&\exists\, a' \cdot a' \in 1..\mathit{size} \rightarrow \mathit{array}[1..\mathit{size}] \\
&\wedge (\forall\, i \cdot i \in 1..\mathit{size} \wedge i \neq \mathit{indice} \wedge i \neq \mathit{indice} + 1 \Rightarrow a'(i) = a(i)) \\
&\wedge a'(\mathit{indice}) = a(\mathit{indice} + 1) \wedge a'(\mathit{indice} + 1) = a(\mathit{indice})
\end{aligned}$$

Here I chose that $a' = a < +\{\mathit{indice} \mapsto a(\mathit{indice} + 1), \mathit{indice} + 1 \mapsto a(\mathit{indice})\}$ (I tried to define the function overriding symbol like in Rodin with $< +$)

After that, the PO was proved automatically.

6.6 BUBBLE_SORT/inv10/INV

Demonstrate:

$$\forall\, i \cdot i \in \mathit{last\_index}..\mathit{size} \wedge i + 1 \in \mathit{last\_index}..\mathit{size} \Rightarrow a(i) \leq a(i + 1)$$

I applied case distinction tactic, with $i = \mathit{last\_index} \vee i > \mathit{last\_index}$, and the PO was proved automatically after that.

6.7 RETURN/grd2/GRD

Demonstrate:

$$\forall\, i \cdot i \in \mathit{dom}(a) \wedge i + 1 \in \mathit{dom}(a) \Rightarrow a(i) \leq a(i + 1)$$

with hypothese:
$(in\_loop = FALSE \wedge swap = FALSE \wedge indice = last\_index \wedge last\_index > 1)$
$\vee\ last\_index = 1$

Apply 'proof by case'-tatic in the hypothese.

6.7.1 First case:

We have:

$(in\_loop = FALSE \wedge swap = FALSE \wedge indice = last\_index \wedge last\_index > 1)$

Then do case distinction for i : $i < last\_index \vee i = last\_index \vee i > last\_index$

In case $i < last\_index$, apply hypothese :
$\forall\, i \cdot i \in 1..last\_index \wedge i + 1 \in 1..last\_index \Rightarrow a(i) \leq a(i + 1)$

In case $i = last\_index$, apply hypothese :
$last\_index < size \Rightarrow (\forall\, i \cdot i \in 1..last\_index \Rightarrow a(i) \leq a(last\_index + 1))$

In case $i > last\_index$, apply hypothese :
$\forall\, i \cdot i \in last\_index + 1..size \wedge i \in last\_index + 1..size \Rightarrow a(i) \leq a(i + 1)$

6.7.2 Second case:

We have: $last\_index = 1$

Apply hypothese :
$\forall\, i \cdot i \in last\_index + 1..size \wedge i + 1 \in last\_index + 1..size \Rightarrow a(i) \leq a(i + 1)$

Then we do case distinction for i : $i = 1 \vee i > 1$

6.8 RETURN/grd3/GRD

Demonstrate :

$$\forall\, i \cdot i \in dom(array) \Rightarrow (\exists\, j \cdot j \in dom(a) \Rightarrow array(i) = a(j))$$

This condition is enough to ensure that no member in **array** is missing in **a**, because the number of occurence of each member is 1. In the next part, sorting a random array, we have to ensure that the number of occurrences of each member in **array** and **a** are the same

6.9 liveness/THM

Apply these hypothese (most of them are logic transformation) :

$$(in\_loop = TRUE \wedge indice < last\_index \wedge a(indice) > a(indice+1) \wedge last\_index > 1) \vee$$
$$(in\_loop = TRUE \wedge indice < last\_index \wedge a(indice) \leq a(indice+1) \wedge last\_index > 1)$$
$$\Leftrightarrow in\_loop = TRUE \wedge indice < last\_index \wedge last\_index > 1$$

$$(in\_loop = TRUE \wedge indice < last\_index \wedge a(indice) > a(indice+1) \wedge last\_index > 1) \vee$$
$$(in\_loop = TRUE \wedge indice < last\_index \wedge a(indice) \leq a(indice+1) \wedge last\_index > 1) \vee$$
$$(in\_loop = TRUE \wedge indice = last\_index \wedge last\_index > 1)$$
$$\Leftrightarrow in\_loop = TRUE \wedge last\_index > 1 \wedge indice \leq last\_index$$

$$(in\_loop = TRUE \wedge indice = last\_index \wedge last\_index > 1) \vee$$
$$(in\_loop = FALSE \wedge swap = FALSE \wedge indice = last\_index \wedge last\_index > 1) \vee$$
$$(in\_loop = FALSE \wedge indice = last\_index \wedge swap = TRUE \wedge last\_index > 1)$$
$$\Leftrightarrow indice = last\_index \wedge last\_index > 1$$

$$(in\_loop = FALSE \wedge swap = FALSE \wedge indice = last\_index \wedge last\_index > 1) \vee$$
$$(in\_loop = TRUE \wedge indice < last\_index \wedge a(indice) > a(indice+1) \wedge last\_index > 1) \vee$$
$$(in\_loop = TRUE \wedge indice < last\_index \wedge a(indice) \leq a(indice+1) \wedge last\_index > 1) \vee$$
$$(in\_loop = TRUE \wedge indice = last\_index \wedge last\_index > 1) \vee$$
$$(in\_loop = FALSE \wedge swap = FALSE \wedge last\_index = size \wedge last\_index > 1) \vee$$
$$(in\_loop = FALSE \wedge indice = last\_index \wedge swap = TRUE \wedge last\_index > 1)$$
$$\Leftrightarrow last\_index > 1 \wedge$$
$$(indice = last\_index \vee in\_loop = TRUE \vee$$
$$(in\_loop = FALSE \wedge swap = FALSE \wedge last\_index = size))$$

7 Sort a radom array

- Specification: SortArrayAscendingMachine

- Implementation: SortArrayAscendingMachineImplementation

The algorithm is still the same as the previous machine, since I used the bubble sort algorithm. But we have 2 more conditions to satisfy, since the array is totally random:

- $dom(new\_array) = dom(array) \land ran(new\_array) = ran(array)$
- $\forall y \cdot y \in ran(array) \Rightarrow card(\{u \mid u \in dom(array) \land u \mapsto y \in array\}) = card(\{x \mid x \in dom(new\_array) \land x \mapsto y \in new_array\})$

That make the appearance of the POs below, which I had to prove interactively :

- INITIALISATION/inv14/INV
- LOOP_SWAP/inv14/INV
- LOOP_SWAP/inv13/INV

To prove the POs, I need to use the following theorem:

- thm5 : $\forall g, n \cdot n \in \mathbb{N} \land g \in 1..n \rightarrow \mathbb{Z} \Rightarrow g = \{i \cdot i \in 1..n \mid i \mapsto g(i)\}$
- thm7 : $\forall g, n \cdot n \in \mathbb{N} \land g \twoheadrightarrow 1..n \rightarrow \mathbb{Z} \Rightarrow g = \{i \cdot i \in 1..n \mid i \mapsto g(i)\}$
- thm8 : $\forall A, B, C \cdot A \subseteq \mathbb{N} \land B \subseteq \mathbb{N} \land C \subseteq \mathbb{N} \land finite(A) \land finite(B) \land finite(C) \land A \cap B = \varnothing \land A \cap C = \varnothing \land B \cap C = \varnothing \Rightarrow card(A \cup B \cup C) = card(A) + card(B) + card(C)$
- thm9 : $\forall A, B \cdot A \subseteq \mathbb{N} \land B \subseteq \mathbb{N} \land A \subseteq B \land finite(A) \land finite(B) \Rightarrow card(A) \leq card(B)$
- thm1 : $\forall f, g, h, k \cdot f \in \mathbb{Z} \twoheadrightarrow \mathbb{Z} \land g \in \mathbb{Z} \twoheadrightarrow \mathbb{Z} \land h \in dom(f) \land k \in dom(f) \land h \neq k \land g = f < +\{h \mapsto f(k), k \mapsto f(h)\} \land finite(f) \land finite(g) \Rightarrow dom(g) = dom(f)$
- thm6 : $\forall g, n, h, k \cdot n \in \mathbb{N} \land g \in 1..n \rightarrow \mathbb{Z} \land h \in dom(g) \land k \in dom(g) \Rightarrow \{h, k\} \lhd g = i \cdot i \in 1..n \land i \neq h \land i \neq k \mid i \mapsto g(i)$
- thm2 : $\forall f, g, h, k, n \cdot n \in \mathbb{N} \land f \in 1..n \rightarrow \mathbb{Z} \land g \in 1..n \rightarrow \mathbb{Z} \land h \in dom(f) \land k \in dom(f) \land h \neq k \land g = f < +\{h \mapsto f(k), k \mapsto f(h)\} \land finite(f) \land finite(g) \Rightarrow ran(g) = ran(f)$
- thm3 : $\forall f, g, h, k, y, n \cdot n \in \mathbb{N} \land f \in 1..n \rightarrow \mathbb{Z} \land g \in 1..n \rightarrow \mathbb{Z} \land h \in dom(f) \land k \in dom(f) \land h \neq k \land g = f < +\{h \mapsto f(k), k \mapsto f(h)\} \land finite(f) \land finite(g) \land y \in ran(f) \Rightarrow card(\{u \cdot u \in dom(f) \land u \mapsto y \in f \mid u\}) = card(\{x \cdot x \in dom(g) \land x \mapsto y \in g \mid x\})$

- thm4 : $\forall f, g, h, k, n \cdot n \in \mathbb{N} \land f \in 1..n \to \mathbb{Z} \land g \in 1..n \to \mathbb{Z} \land h \in dom(f) \land k \in dom(f) \land h \neq k \land finite(f) \land finite(g) \land (\forall i \cdot i \in 1..n \land i \neq h \land i \neq k \Rightarrow g(i) = f(i)) \land g(h) = f(k) \land g(k) = f(h) \Rightarrow g = f < +\{h \mapsto f(k), k \mapsto f(h)\}$

7.1 INITIALISATION/inv14/INV

Demonstrate that : $finite(array)$
By point out that : $\exists f \cdot f \in 1..size \rightarrowtail\!\!\!\!\rightarrow array$
I chose $f = \{i \cdot i \in 1..size \mid i \mapsto (i \mapsto array(i))\}$, and then I repeat the removal of $\in$ in goal to simplify the PO.

7.2 LOOP_SWAP/inv14/INV

Demonstrate that : $finite(a')$
The process is the same as above, except that this time, I used the hypothese added to make the proving more easier :
$\{i \cdot i \in 1..size \mid i \mapsto a'(i)\} = a'$

7.3 LOOP_SWAP/inv13/INV

Demonstrate that :
$\forall y \cdot i \in ran(array) \Rightarrow card(\{u \cdot u \in dom(array) \land u \mapsto y \in array \mid u\}) = card(\{x \cdot x \in dom(a') \land x \mapsto y \in a' \mid x\})$

Use the hypothese : $card(\{u \cdot u \in dom(array) \land u \mapsto y \in array \mid u\}) = card(\{x \cdot x \in dom(a) \land x \mapsto y \in a \mid x\})$.
We then need to prove :
$card(\{x \cdot x \in dom(a') \land x \mapsto y \in a' \mid x\}) = card(\{u \cdot u \in dom(a) \land u \mapsto y \in a \mid u\})$
Use the **thm4** to precise that $a' = a < +\{indice \mapsto a(indice + 1), indice + 1 \mapsto a(indice)\}$
Then use **thm3** to demonstrate $card(\{x \cdot x \in dom(a') \land x \mapsto y \in a' \mid x\}) = card(\{u \cdot u \in dom(a) \land u \mapsto y \in a \mid u\})$

Now the main point is, to prove all the added theorem.**thm1**, **thm5**, **thm7**, **thm9** are pretty much auto proved.

7.4 thm8/THM

This theorem is proved by using the original formular of $card(A \cup B \cup C)$, and the fact that intersection between A, B or C is empty.

7.5 thm6/THM

This theorem is proved by adding :
$\{h, k\} \lhd g = \{j \cdot j \in dom(g) \setminus \{h, k\} \mid j \mapsto g(j)\}$

7.6 thm2/THM

This theorem was proved by re-define the overriding operartion, and then apply **thm6**, and then apply the classic process :
$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$
After re-define the overriding operation, we get the new PO :
$ran((\{h, k\} \lhd f \cup \{h \mapsto f(k), k \mapsto f(h)\})) = ran(f)$
This proposition $ran((\{h, k\} \lhd f \cup \{h \mapsto f(k), k \mapsto f(h)\})) \subseteq ran(f)$ is proved automatically. We need to prove :
$ran(f) \subseteq ran((\{h, k\} \lhd f \cup \{h \mapsto f(k), k \mapsto f(h)\}))$
This is proved by point out : $\forall x0 \mapsto x \in f$, we prove that $x \in ran((\{h, k\} \lhd f \cup \{h \mapsto f(k), k \mapsto f(h)\}))$
By using case distinction : $x0 = h \vee x0 = k \vee (x0 \neq h \wedge x0 \neq k)$, we can prove this easily.

7.7 thm4/THM

This theorem is proved by demonstrate 2 propositions :

- $g \subseteq f < +\{h \mapsto f(k), k \mapsto f(h)\}$
- $f < +\{h \mapsto f(k), k \mapsto f(h)\} \subseteq g$

Then apply **thm5** on each side, and then divide after $dom(f)$ and $\{h, k\}$.

7.8 thm3/THM

This theorem is the main point, that lead to the demonstration of **LOOP_SWAP/inv13/INV**.

To do this, there're somethings we need to pay attention :
$\forall y \in rang(f) \cdot \{u \cdot u \in 1..n \wedge u \mapsto y \in f \mid u\} = \{u \cdot u \in 1..n \wedge u \neq h \wedge u \neq k \wedge u \mapsto y \in f \mid u\} \cup \{u \cdot u = h \wedge u \mapsto y \in f \mid u\} \cup \{u \cdot u = k \wedge u \mapsto y \in f \mid u\}$
We have 3 new subsets, and intersection between each pair, is null. Apply **thm8** for both f and g 's side. Then prove the followings :

- $card(\{u \cdot u \in 1..n \wedge u \neq h \wedge u \neq k \wedge u \mapsto y \in f \mid u\}) = card(\{u \cdot u \in 1..n \wedge u \neq h \wedge u \neq k \wedge u \mapsto y \in g \mid u\})$
- $card(\{u \cdot u = h \wedge u \mapsto y \in f \mid u\}) = card(\{u \cdot u = k \wedge u \mapsto y \in g \mid u\})$
- $card(\{u \cdot u = k \wedge u \mapsto y \in f \mid u\}) = card(\{u \cdot u = h \wedge u \mapsto y \in g \mid u\})$