Sorting

Arthur Ryman, arthur.ryman@gmail.com

August 5, 2021

Abstract

This article formalizes the notion of sorting to illustrate the relation between a specification and an implementation, and how to prove that an implementation satisfies a specification.

1 Sorting

Suppose we are given a finite list of numbers and are asked to sort it. By sorting we mean that the result should contain exactly the same set of numbers, with the same multiplicities, arranged in ascending order.

1.1 Lists, *LIST*

Let *LIST* denote a finite sequence of integers.

$$LIST == \operatorname{seq} \mathbb{Z}$$

1.2 Ascending Order *ascending*

A list is in ascending order when any element that appears earlier in the list is less than or equal to any element that appears later in the list. Let *ascending* denote the set of all lists that are in ascending order.

$$ascending == \{ s : LIST \mid (\forall i, j : \operatorname{dom} s \mid i < j \bullet s(i) \leq s(j)) \}$$

Although mathematically correct, the definition of *ascending* is not in a form that can be implemented efficiently on a computer. The definition implies that if the list contains n elements then there are $n(n+1)/2$ pairs (i, j) such that $i \leq j$ for which s has to be checked. The complexity of the direct, naive implementation of this check is therefore $O(n^2)$. Clearly, we can reduce this complexity to $O(n)$.

1.3 Refinement of Ascending Order $\mathit{ascending}1$

A more efficient definition of ascending order is given by $\mathit{ascending}1$.

$$\mathit{ascending}1 == \{\, s : \mathit{LIST} \mid (\forall\, i : \operatorname{dom} s \mid i < \#s \bullet s(i) \leq s(i+1)) \,\}$$

Clearly, a direct implementation of this definition has complexity $O(n)$.

1.4 Theorem $\mathit{ascending} = \mathit{ascending}1$

Although the equivalence of *ascending* and *ascending*1 is obvious to a human, other similar optimizations may not be. It is therefore instructive to prove the equivalence.

The plan of the proof is to prove $\mathit{ascending} \subseteq \mathit{ascending}1$ and $\mathit{ascending}1 \subseteq \mathit{ascending}$ which corresponds to unfolding the definition of equality for sets.

First prove $\mathit{ascending} \subseteq \mathit{ascending}1$.

$s : \mathit{ascending}$	[assumption]
$\forall\, i, j : \operatorname{dom} s \mid i < j \bullet s(i) \leq s(j)$	[def of *ascending*]
$i : \operatorname{dom} s \mid i < \#s$	[intro i]
$j == i + 1$	[intro j]
$j \in \operatorname{dom} s$	[def of dom]
$i < j$	[def of $<$]
$s(i) \leq s(j)$	[$\forall$-elim]
$s(i) \leq s(i+1)$	[def of j]
$\forall\, i : \operatorname{dom} s \mid i < \#s \bullet s(i) \leq s(i+1)$	[$\forall$-intro]
$s \in \mathit{ascending}1$	[def of *ascending*1]
$s : \mathit{ascending} \Rightarrow s \in \mathit{ascending}1$	[$\Rightarrow$-intro]
$\mathit{ascending} \subseteq \mathit{ascending}1$	[s-elim QED]

Next prove $\mathit{ascending}1 \subseteq \mathit{ascending}$. This proof requires induction on the length of the list.

$s : \mathit{ascending}1$	[assumption]
$\forall\, i : \operatorname{dom} s \mid i < \#s \bullet s(i) \leq s(i+1)$	[def of *ascending*1]