TD10 – Hoare Logic

simon.castellan@ens-lyon.fr

***Exercise* 1** (Warmup). — 1. Write down *carefully* the full derivation of

$$\{x = n \land y = m\}\ \texttt{z:=x ; x:=y ; y:=z}\ \{x = m \land y = n\}$$

according to the rules of Hoare Logic.

2. What is the meaning of:

   (a) $\vdash \{\bot\}\texttt{c}\{A\}$?
   (b) $\vdash \{A\}\texttt{c}\{\top\}$?
   (c) $\vdash \{\top\}\texttt{c}\{A\}$?
   (d) $\vdash \{A\}\texttt{c}\{\bot\}$?

***Exercise* 2** (Dijkstra's Dutch National Flag). — Suppose that memory locations can take colors `Red`, `White` and `Blue` as values (they can be encoded with numbers, if you prefer). Also consider an extension of the language of Hoare Logic, where you have arrays, i.e. finite lists of memory locations. Given an array a, you can express the length $\mathit{length}(a)$ of a and for each $i \leq \mathit{length}(a)$ you can refer to the ith memory location with $a[i]$.

1. Write an **IMP** program `DNF` which sorts an array of memory locations in such a way that it resembles the Dutch national flag (ie. it is sorted wrt the order `Red` < `White` < `Blue`).

2. Formalize the specification in terms of pre- and post-conditions A and B. Argue that

$$\vdash \{A\}\ \texttt{DNF}\ \{B\}$$

   holds.

3. In order to judge how good is your invariant A, think of the following 'buggy' implementation `DNF'` of the 'Dutch National Flag' specification: given the input array $x_1, \ldots, x_n$, behave as `DNF` if $n < 3$, otherwise write `Red` in x_1, `White` in x_2 and `Blue` in $x_3, \ldots, x_n$. Does it satisfy A at the beginning and B at the end of the execution? Can you think of different As and Bs which rule out `DNF'`, i.e. such that

$$\nvdash \{A\}\ \texttt{DNF'}\ \{B\}?$$

   This should make you reflect on expressiveness of Hoare Logic.

***Exercise* 3** (Total Correctness). — How to modify Hoare logic to prove total correctness instead of partial correctness?

***Exercise* 4** (Exceptions). — Consider the extension of Imp with two constructions: $\texttt{raise}\alpha$ and $\texttt{trap}\ \alpha\ \texttt{in}\ C_1\ \texttt{with}\ C_2$.

1. Explain how to extend the denotational semantics by continuation of Imp to these constructs.

2. Deduce new rules for the axiomatic semantics.

3. Prove the correctness of this new system.