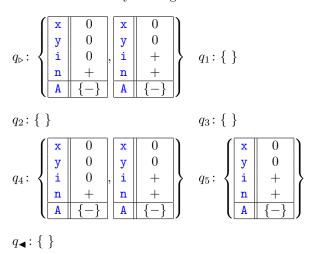
## 02141 Computer Science Modeling Solutions to Selected Exercises from Formal Methods Appetizer, Chapter 4

**Exercise 4.11** Solution: A correct analysis assignment A' is the following:



Note that  $\mathbf{A}'(q_{\blacktriangleleft}) = \emptyset$  since  $\mathbf{y}$  has sign 0 in all abstract memories of  $q_5$  and division by zero is assumed to be undefined. The analysis assignment is correct (Definition 4.6) with respect to the initial memory  $\mathsf{Mem}_{\triangleright} = \{\sigma\}$  and semantics  $\mathcal{S}$  (see e.g. Definition 2.17) where  $\sigma(\mathbf{x}) = \sigma(\mathbf{y}) = \sigma(\mathbf{i}) = 0$ ,  $\sigma(\mathbf{n}) > 0$ , and in which the values of the elements in  $\mathbf{A}$  are negative, because:

- 1. The abstract memory  $\eta(\sigma)$  of the initial memory  $\sigma$  is in  $\mathbf{A}'(q_{\triangleright})$ .
- 2. For each of the edges  $(q_1, q_2), (q_2, q_3), (q_3, q_{\triangleright})$  the analysis assignments of the source nodes are all empty. Hence Definition 4.6 is vacuously true for those edges.
- 3. For the edge e from  $q_{\triangleright}$  to  $q_1$  correctness is satisfied since  $\mathcal{S}[\![\mathsf{action}(e)]\!]\sigma$  is undefined for any  $\sigma$  such that its abstraction is in  $\mathbf{A}'(q_{\triangleright})$ . Hence the analysis assignment is vacuously correct for the source node of this edge as well.
- 4. For the edge e from  $q_{\triangleright}$  to  $q_5$  only the abstract states of  $\mathbf{A}'(q_{\triangleright})$  in which  $\mathbf{i}$  has sign + will occur in  $\mathbf{A}'(q_5)$ , since  $\mathbf{n}$  has sign + in every abstract memory of  $\mathbf{A}'(q_{\triangleright})$ .
- 5. For the edge e from  $q_5$  to  $q_{\blacktriangleleft}$  the sign of y is 0 in all abstract memories of the source node. Hence  $\mathcal{S}[[action(e)]]\sigma$  is undefined for any memory  $\sigma$  whose abstraction is in  $\mathbf{A}'(q_5)$ . Hence the analysis assignment is vacuously correct for  $q_{\blacktriangleleft}$  as well.

- 6.  $\mathbf{A}'(q_4) = \mathbf{A}'(q_{\triangleright})$  since  $\mathcal{S}[[action(e)]]\sigma = \sigma$  on the only incoming edge e of  $q_4$  from  $q_{\triangleright}$  to  $q_4$ , for any  $\sigma$  whose abstraction is in  $q_{\triangleright}$ .
- 7. The edge from  $q_4$  to  $q_{\triangleright}$  increments  $\mathbf{i}$ . Hence  $\mathbf{A}'(q_{\triangleright})$  contains the abstract memories of  $\mathbf{A}'(q_4)$  in which the sign of  $\mathbf{i}$  has been changed to +.