Final Exam Study Guide
Open book/notes

Time: Monday May 8, 2:15 – 4:15 pm

Location: 114 MLH

Major topics (comprehensive):

- * logic (Diller, chaps. 3, 10)
  - truth analysis and models
  - proof and deduction
  - consistency and completeness
- * program proving (Diller, chap. 14)
- * Z specification
  - specification elements (Diller, chaps. 4, 16, 18)
  - Z Library (Diller, chap. 21 augmented by chaps. 3, 5, 6 & 7)
  - animation/Miranda/Zans (Diller, chap. 19)
- * algebraic specification (Guttag/Horowitz/Musser & Horabeek/Lewi)
  - initial vs. final algebra semantics
  - consistency and sufficient completeness
  - animation/Miranda
  - errors (i.e., exceptions) and order-sorted algebras
- * statecharts (Harel/Gery & chap 2 of Day)

Final Exam Study Questions

Since the exam is comprehensive, one useful step is to review the midterm and homework problems. Of course, timed exam questions are necessarily formulated to have much briefer answers than homework problems, but the homework is topically representative. A few additional selected problems appear below.

Below is a program fragment to compute the *index* J of a minimum item of an array A[1..N] of numbers — this is expressed in logic as the post-condition shown. Use the Floyd-Hoare axiomatic rules to prove that the formula

$1 \le J \le K \le N \wedge (1 \le L \le K \Rightarrow A[J] \le A[L])$

is a loop invariant.

```
      {N≥1}
  J:= 1;  K:= 1;
  while K<N do
  begin
  K:= K+1;  if A[K] < A[J] then J:= K else skip
  end
{1≤J≤N ∧ (1≤L≤N ⇒  A[J]≤A[L])}
```

Problem 5.2, p. 89 of Diller.

Both bags and sequences in Z consist of sets of ordered pairs, and therefore share basic set operations. Indicate whether each of the following is *true or false*, and justify your answer.

(a) for any sequences, S prefix T ⇔ S □ T (recall that the prefix relation is defined for sequences S,T: seq X as: S prefix T ⇔ (□V: seq X • S^V = T)),

(b) for bags B and C, bag difference and set difference are the same, B □ C = B \ C.

When we illustrated "OK tests" to treat exceptional conditions on the Queue ADT (repeated below), a number of things changed. Compare in detail the ground term equivalence classes that result in the specification including exceptions with those obtained from the Queue specification of Guttag et al.

• Signature

New: $\rightarrow$ Queue
$\text{Error}_{\text{Que}}$: $\rightarrow$ Queue
Add: Queue $\times$ Int $\rightarrow$ Queue
Del: Queue $\rightarrow$ Queue
Frt: Queue $\rightarrow$ Int
IsNew: Queue $\rightarrow$ Boolean
OK: Queue $\rightarrow$ Boolean

• OK specification

OK(New) = True
OK($\text{Error}_{\text{Que}}$) = False
OK(Add(q,i)) = OK(q) $\wedge$ OK(i)

• Error-equations (this is “errors propagate” plus two additional equations)

Add($\text{Error}_{\text{Que}}$,i) = $\text{Error}_{\text{Que}}$
Add(q,$\text{Error}_{\text{Int}}$) = $\text{Error}_{\text{Que}}$
Del(New) = $\text{Error}_{\text{Que}}$
Del($\text{Error}_{\text{Que}}$) = $\text{Error}_{\text{Que}}$
Frt(New) = $\text{Error}_{\text{Int}}$
Frt($\text{Error}_{\text{Que}}$) = $\text{Error}_{\text{Int}}$
IsNew($\text{Error}_{\text{Que}}$) = $\text{Error}_{\text{Bool}}$

• OK-equations

IsNew(New) = True
IsNew(Add(q,i)) = **if** OK(q) $\wedge$ OK(i)
    then False **else** $\text{Error}_{\text{Bool}}$
Del(Add(q,i)) = **if** OK(q) $\wedge$ OK(i)
    then if IsNew(q) **then** New **else** Add(Del(q),i)
    else $\text{Error}_{\text{Que}}$
Frt(Add(q,i)) = **if** OK(q) $\wedge$ OK(i)
    then if IsNew(q) **then** i **else** Frt(q)
    else $\text{Error}_{\text{Int}}$

Queue with Errors

In class, we observed that the example traffic light statechart from Day's thesis permits the configuration where both N_S and E_W lights are simultaneously green. A revision of this specification to prevent this error is presented in the figure below by changing the condition for the transition t2 in N_S from Red to Green to en(E_W.RED). With this change, transition t2 is only triggered when E_W.RED was entered in the immediately preceding step. However, this "corrected" version still fails — show what the failure is, and suggest and justify a correction.