2G1516 Formal Methods

Examination Problems — *Mads Dam*
20 December 2005, 2pm–7pm — KTH/IMIT

> Give solutions in English or Swedish, each problem beginning on a new sheet. Write your name on all sheets. The maximal number of points is given for each problem. Textbook, copies of slides, other written course material and English dictionaries are admissible. Computers, mobile phones, other computing or communication equipment, is not.
> Grades are given in the range F, 3, 4, 5 with the following cut-off points: 3: 50, 4: 70, 5: 85

---

1. A distributed file manager application needs to lock a semaphore for a write operation to succeed. The specification uses the events P, V, *WriteReq*, *WriteSuccess*, and *WriteFail*. A write operation is considered bounded by two events: a *WriteReq* event starts the write operation and either a *WriteSuccess* or a *WriteFail* event ends it. A successful write operation is a write operation ending in *WriteSuccess*. Say also that the semaphore is *free*, or *released*, if the most recent operation applied to it was V, and say it is *busy* if it is not free. Express in LTL the following properties: **20p**

   1. Any *WriteReq* event is followed some time later by either a *WriteSuccess* or a *WriteFail*.
   2. The (current) event *WriteReq* starts a successful write operation.
   3. It is not possible to start a successful write operation unless the semaphore is busy.
   4. If a successful write operation is started, the semaphore cannot be released before the write operation is completed.
   5. A successful write operation can take place only when the semaphore is busy throughout it.

---

2. Produce an LTL formula corresponding to the Buchi automaton in figure 1. **15p**

---

3. A language $L \subseteq \Sigma^\omega$ is *1-recognizable* if there is a Buchi automaton $A = (Q, \Sigma, \Delta, I, F)$ such that $|F| = 1$ and $L = L(A)$. Prove that each Buchi recognizable language $L \subseteq \Sigma^\omega$ can be written as a finite union of 1-recognizable languages, i.e. there are 1-recognizable languages $L_1, \ldots, L_n$ such that $L = L_1 \cup \cdots \cup L_n$. **15p**

Please Turn Over

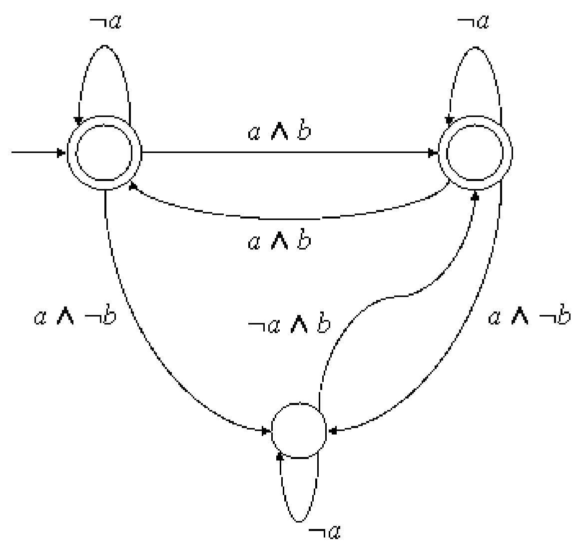

Figure 1: Buchi automaton for question 2

---

4. Let P be the program `cobegin` $x := x+1 \parallel x := x+2$ `coend`. Prove the Hoare triple $\{x=0\}P\{x=3\}$. **20p**

---

5. Let $X == \tau.X+\tau.a.0$, and $Y == \tau.Y+a.0$. For each combination of processes $P, Q \in \{a.0, X, Y\}$ determine whether or not P and Q are (a) weakly bisimilar, and (b) observationally congruent. Justify your answer by either providing a suitable relation, or argue why no such relation can exist. **15p**

---

6. Define the CCS processesc$S == \tau.b.S$, $P == \overline{a}.b.P + b.P$, $Q == a.Q$, and $I == (P \mid Q)\backslash\{a\}$. Using the laws for observational congruence prove $S = (P \mid Q)\backslash\{a\}$. **15p**

Good luck!