12 Hoare Logic and Model Checking (AM)

(*a*) Suppose we have a representation of a computer system, either as a set of axioms Γ specifying its behaviour or as a model $\mathcal{M}$, along with a property ϕ which we expect to hold (but which may not hold due to programming errors). Give two reasons why we might prefer to model-check $\mathcal{M} \models \phi$ rather than use logical inference to prove $\Gamma \vdash \phi$. [2 marks]

(*b*) Assuming a given set AP of atomic properties, ranged over by p, give the syntax of LTL formulae ϕ. (It is not necessary to be encyclopaedic—full marks can be obtained by including four constructs not present in classical logic.) Explain how an LTL formula is interpreted as true or false in a model. It suffices to consider two temporal operators along with conjunction and an atomic property p. [7 marks]

(*c*) Suppose p is an atomic property. Give informal explanations of the two properties $\mathbf{G}(\mathbf{F}\ p)$ and $\mathbf{F}(\mathbf{G}\ p)$. State, giving reasons, whether the properties are equivalent or whether one implies the other. [3 marks]

(*d*) Consider a program consisting of the following two threads where `WORK` is an unspecified unit of work not involving variables `A` or `B`. The threads are executed on a scheduler which first sets `A` and `B` to zero and then repeatedly and non-deterministically chooses to execute a *whole line* of code from either the left or right thread. An `AWAIT` e statement can only be scheduled if its condition e evaluates to true.

```
L:  AWAIT A=0;  A:=1;        | M:  AWAIT B=0;  B:=1;
    AWAIT B=0;  B:=1;        |     AWAIT A=0;  A:=1;
    WORK;                    |     WORK;
    A:=0; B:=0; GOTO L;      |     B:=0; A:=0; GOTO M;
```

Determine a Kripke structure model for this program, and draw it as a finite-state automaton. You should label one or more states of the automaton as satisfying the atomic property of `deadlock`. [5 marks]

(*e*) Give a temporal logic formula expressing that `deadlock` does not occur. For the program in Part (*d*), would a model checker prove this formula or produce a counterexample trace? [3 marks]