Formal Methods in Software Development

Written/Oral Test – Rome, July 14, 2020

Name
Surname

1. Modelling

Q1: Why does the parallel composition of n processes give rise to a Labeled Transition System (or a Kripke structure) with a number of states exponential in n?

Q2 Give the definition of a Kripke structure.

Q3 Why Kripke structures are not suitable to model synchronisation of concurrent systems?

Q4 Explain what does "interleaving semantics" mean in the parallel composition of concurrent systems.

Q5 Why computations (or runs) in kripke structures consists always of an infinite number of steps?

Q6 Could you sketch how a Kriepke structure can be modeled using boolean predicates?

Temporal Logic

Q1 Give a Kripke structure $\mathcal{M}$ (as small as possible) and a state s such that $\mathcal{M}, s \models \mathbf{A}\ \mathbf{G}\ \mathbf{F}a$, where a is an atomic proposition.

Q2 Write a formula equivalent to $\mathbf{F}f$ containing the temporal operator $\mathbf{U}$ only.

Q3 Write a formula equivalent to $\mathbf{F}f$ containing the temporal operator $\mathbf{G}$.

Q4 Write the expansion law for the temporal operator $\mathbf{U}$, that is a formula equivalent to $f\ \mathbf{U}\ g$ in terms of operators $\mathbf{X}$ and $\mathbf{U}$ itself.

Linear Time Properties

Q1 Define a safety property.

Q2 Define a liveness property.

Q3 Can you give an example of a property that is simultaneously a safety and a liveness property?

Q4 Define an invariant and describe a model checking procedure for an invariant.

Fixed Points

Q1 Let S be a set and $T : 2^S \mapsto 2^S$. Give sufficient conditions on T so that T has a least fixpoint.

Q2 Let S be a set and $T : 2^S \mapsto 2^S$ defined by $T(X) = S \setminus X$. Has T a fixpoint? Motivate your answer.

Q3 Let $G = (V, E)$ be a directed graph and $u \in V$. Let $T : 2^V \mapsto 2^V$ defined by $T(X) = \{u\} \cup \{v \mid y \to v \in E, \text{for some } y \in X\}$. Has T a minimum fixed point? If yes, which is the fixpoint of T?

Q4 Let S be a *finite* set and let $a \in S$. Which are the least and the greatest fixed points of the operator $T : 2^S \mapsto 2^S$ defined by: $T(X) = X \cup \{a\}$?

Automata

Q1 Which is the difference between a Büchi automata and Finite State automata?

Q2 Is the class of Deterministic Büchi automata equivalent to the class of Nondeterministic Büchi automata?

Q3 Let $G = (V, E)$ be a directed graph and $u \in V$. Let $T : 2^V \mapsto 2^V$ defined by $T(X) = \{u\} \cup \{v \mid y \to v \in E, \text{for some } y \in X\}$. Has T a minimum fixed point? If yes, which is the fixpoint of T?

Q4 Let S be a *finite* set and let $a \in S$. Which are the least and the greatest fixed points of the operator $T : 2^S \mapsto 2^S$ defined by: $T(X) = X \cup \{a\}$?

OBDDs

Q1 Could you sketch how a Kriepke structure can be modeled as boolean predicates?

Q2 Could you provide an example of a n-ary boolan function f and two variable orders $\leq_1$ and $\leq_2$ such that the OBDD representing f is linear in n by considering the variable order $\leq_1$ and exponential in n by considering the variable order $\leq_2$?

Q2 If you have an OBDD representing the boolan function f, how you can compute the OBDD representing $\sim f$?

Algorithms:

Q1 Briefly describe the (idea of the) procedure *checkEU(f,g)* that labels all states satisfying $\mathbf{E}[f \ \mathbf{U} \ g]$, assuming that states satisfying f and g are correctly labeled.

Q2 Briefly describe the (idea of the) procedure *checkEG(f)* that labels all states satisfying $\mathbf{E}[\ \mathbf{G} \ f]$, assuming that states satisfying f are correctly labeled.

Equivalences

Q1 Among the following temporal logics, which ones are always invariant with respect to stuttering equivalence?

☐ LTL$_{-\mathbf{X}}$
☐ CTL$_{-\mathbf{X}}$
☐ CTL

□ LTL