Hoare Logic and Model Checking – additional slides

Alan Mycroft

Computer Laboratory, University of Cambridge, UK
http://www.cl.cam.ac.uk/~am21

CST Part II – 2015/16

Revision

[1A Digital Electronics and 1B Logic and Proof]

- Are $AB + A\overline{C} + BC$ and $BC + A\overline{C}$ equivalent?
- In other words, letting ϕ be the formula
  $(A \wedge B) \vee (A \wedge \neg C) \vee (B \wedge C) \quad \Leftrightarrow \quad (B \wedge C) \vee (A \wedge \neg C)$
  does $\models \phi$ hold (in propositional logic)?
- Two methods:
  - we could show $\models_M \phi$ for every model M
  - we could prove $\vdash_R \phi$ for some set of sound and complete set of rules R (e.g. algebraic equalities like $A \vee (A \wedge B) = A$)
- So far in the course we've used $\vdash$. But for propositional logic (e.g. hardware) it's easier and faster to check that $\models_M \phi$ holds in all eight models. Why? Finiteness. (Note that Karnaugh maps can speed up checking this.)
- Additional benefit: counter-example if something isn't true.

Revision (2)

- A model for propositional logic with propositional variables $\{A, B, C\}$ is just that subset of $\{A, B, C\}$ which are to be considered true. Let P range over propositional variables.
- When does a formula ϕ satisfy a model? Defined by structural induction on ϕ:
- $$\begin{array}{ll} \models_M P & \text{if } P \in M \\ \models_M \neg\phi & \text{if } \models_M \phi \text{ is false} \\ \models_M \phi \wedge \phi' & \text{if } \models_M \phi \text{ and } \models_M \phi' \end{array}$$
- Sometimes write $[\![\phi]\!]_M$ for this (only an incidental connection to denotational semantics). So the above becomes (e.g.)
  $$[\![P]\!]_M = \begin{cases} \mathit{true} & \text{if } P \in M \\ \mathit{false} & \text{if } P \notin M \end{cases}$$
  $$[\![\neg\phi]\!]_M = \text{not } [\![\phi]\!]_M$$
  $$[\![\phi \wedge \phi']\!]_M = [\![\phi]\!]_M \text{ and } [\![\phi']\!]_M$$

Differences in this course

- In this course we write $M \models \phi$ (and sometimes $[\![\phi]\!]_M$) rather than the $\Gamma \models_M \phi$ of Logic and Proof.
- In this course we're mainly interested in whether a formula ϕ holds in some particular model M, not in all models.
- We're also interested in richer formulae than propositional logic and richer models than "which propositional variables are true", because we're interesting in time (hence the name "temporal logic").