Logics of Programs	Final Exam Solutions
CS686 Spring 2001	Friday, May 25

1. If $bp = pc$, then $bp\overline{c} + \overline{b}pc = pc\overline{c} + \overline{b}bp = 0 + 0 = 0$.

   Conversely, if $bp\overline{c} + \overline{b}pc = 0$, then both $bp\overline{c} = 0$ and $\overline{b}pc = 0$. As argued in class, $bp\overline{c} = 0$ is equivalent to $bp = bpc$, and symmetrically, $\overline{b}pc = 0$ is equivalent to $pc = bpc$. Thus $bp = pc$.

   The property $bp = pc$ is often used in practice in place of the Hoare assignment rule $\{\varphi[x/e]\}\ x := e\ \{\varphi\}$. Recall that if we take $b = \varphi[x/e]$, $c = \varphi$, and $p = x := e$, then the Hoare rule is equivalent to $bp\overline{c} = 0$ or $bp = bpc$. This is half of the property above. The other half, namely $\overline{b}pc = 0$, is equivalent to $\overline{b}p = \overline{b}p\overline{c}$, which corresponds to $\{\neg\varphi[x/e]\}\ x := e\ \{\neg\varphi\}$. Thus the equation $bp = pc$ is equivalent to two applications of the Hoare assignment rule, one to φ and one to its negation.

2. The KAT representations of the two programs are $(bp)^*\overline{b}(cq(bp)^*\overline{b})^*\overline{c}$ and $((b+c)(bp+\overline{b}(cq+\overline{c})))^*\overline{b+c}$, respectively. Simplifying the former program,

$$\begin{aligned}(bp)^*\overline{b}(cq(bp)^*\overline{b})^*\overline{c} &= (bp)^*(\overline{b}cq(bp)^*)^*\overline{b}\overline{c} \\ &= (bp+\overline{b}cq)^*\overline{b}\overline{c}.\end{aligned}$$

   The first step uses the sliding rule $(pq)^*p = p(qp)^*$ and the second uses the denesting rule $p^*(qp^*)^* = (p+q)^*$. Simplifying the latter program,

$$\begin{aligned}((b+c)(bp+\overline{b}(cq+\overline{c})))^*\overline{b+c} &= (bbp + b\overline{b}cq + b\overline{b}\overline{c} + cbp + c\overline{b}cq + c\overline{b}\overline{c})^*\overline{b}\overline{c} \\ &= (bp + bcp + \overline{b}cq)^*\overline{b}\overline{c} \\ &= (b(1+c)p + \overline{b}cq)^*\overline{b}\overline{c} \\ &= (bp + \overline{b}cq)^*\overline{b}\overline{c}.\end{aligned}$$

3. Denote $\varphi[X/\psi]$ by $\varphi(\psi)$ and $\varphi(\varphi(\psi))$ by $\varphi^2(\psi)$. Let $A = \mu X.\varphi(X)$ and $B = \mu X.\varphi^2(X)$. We wish to show that A and B are equivalent. The rules for μ are

$$\varphi(\mu X.\varphi(X)) \to \mu X.\varphi(X) \tag{1}$$

$$\frac{\varphi(\psi) \to \psi}{\mu X.\varphi(X) \to \psi}. \tag{2}$$

   We also use a monotonicity rule, which says that if $\psi \to \rho$, then $\varphi(\psi) \to \varphi(\rho)$, provided all free occurrences of X in φ are positive. The soundness of this rule is easily established by induction on the structure of φ.

Here is a proof of $B \to A$. Starting with $\varphi(A) \to A$, which is an instance of (1),

$$\cfrac{\cfrac{\cfrac{\varphi(A) \to A}{\varphi^2(A) \to \varphi(A)}\ \text{monotonicity}}{\varphi^2(A) \to A}\ \text{(1) and transitivity of} \to}{B \to A}\ (2)$$

Here is a proof of $A \to B$. Starting with $\varphi^2(B) \to B$, which is an instance of (1),

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\varphi^2(B) \to B}{\varphi^3(B) \to \varphi(B)}\ \text{monotonicity}}{B \to \varphi(B)}\ (2)}{\varphi(B) \to \varphi^2(B)}\ \text{monotonicity}}{\varphi(B) \to B}\ \text{(1) and transitivity of} \to}{A \to B}\ (2)$$

4. (a) The 3-state Büchi automaton with states $\{0, 1, X\}$, transitions

$$(1, a, 0, 0),\ (1, b, 1, 0),\ (1, b, 0, 1),$$
$$(0, a, X, X),\ (0, b, 0, 0),$$
$$(X, a, X, X),\ (X, b, X, X),$$

start state 1, and final states $\{0\}$ does it. Intuitively, state $i \in \{0, 1\}$ means, "I would like to see exactly i a's in the subtree rooted at my current position," and X means failure.

On any tree with exactly one node n labeled a, label n and all its ancestors with 1, and label all other nodes 0; this is an accepting run. Conversely, any accepting run must have a node n such that n and all its ancestors are labeled 1, and all other nodes are labeled 0; any labeling not of this form violates one of the conditions of an accepting run. Then n and no other node can be labeled a.

(b) Suppose there were a deterministic Muller automaton M accepting this set. Let n and m be any two nodes, neither of which is an ancestor of the other. Let T_n (resp., T_m) be the tree that labels n (resp., m) with a and all other nodes with b. Let $T_{n,m}$ be the tree that labels both n and m with a and all other nodes with b. Let ρ_n and ρ_m be the (unique) accepting runs of M on T_n and T_m, respectively. Then the run

$$\rho_{m,n}(x) = \begin{cases} \rho_n(x), & \text{if } x \text{ is } n \text{ or a descendant of } n \\ \rho_m(x), & \text{otherwise} \end{cases}$$

is an accepting run of $T_{m,n}$, thus $T_{m,n}$ is erroneously accepted.

The complementation lemma proved in class implies that there exists a nondeterministic Rabin or Muller automaton accepting the complement of this set. In fact, there is a nondeterministic Büchi automaton with 6 states. Can you produce it?

5. (a) The complete binary tree K with $\mathfrak{m}_K(p) = 0^*1$ has no path with infinitely many nodes satisfying p, yet there is no bound on the depth of such nodes.

(b) Recall from class that the PDL formula $\texttt{<}a^*\texttt{>}\varphi$ is expressed $\mu X.(\varphi \vee \texttt{<}a\texttt{>}X)$ in the μ-calculus. Let $a^+ = a^*a$. Then

$$\begin{aligned}\texttt{<}a^+\texttt{>}\psi &\leftrightarrow \texttt{<}a^*\texttt{><}a\texttt{>}\psi \\ &\leftrightarrow \mu Y.(\texttt{<}a\texttt{>}\psi \vee \texttt{<}a\texttt{>}Y) \\ &\leftrightarrow \mu Y.\texttt{<}a\texttt{>}(\psi \vee Y).\end{aligned}$$

Thus the complement of $\mu X.\nu Y.\texttt{[}a\texttt{]}((X \vee \neg p) \wedge Y)$, namely $\nu X.\mu Y.\texttt{<}a\texttt{>}((X \wedge p) \vee Y)$, is equivalent to $\varphi = \nu X.\texttt{<}a^+\texttt{>}(X \wedge p)$. It therefore suffices to show that $s \vDash \varphi$ iff there exists a path through s with infinitely many states satisfying p.

If s satisfies φ, then s satisfies $\texttt{<}a^+\texttt{>}(\varphi \wedge p)$, which says that there is a proper descendant s_1 of s satisfying p and φ. Repeating the argument at s_1, we obtain a proper descendant s_2 of s_1 satisfying p and φ, and so on. This gives an infinite path through s with infinitely many states s_i satisfying p.

Conversely, if there is a path through s with infinitely many states satisfying p, let A be the set of states on that path. Then $A \subseteq \texttt{<}a^+\texttt{>}(A \wedge p)$, so A is a postfixpoint of the operator $X \mapsto \texttt{<}a^+\texttt{>}(X \wedge p)$. Since φ is the greatest postfixpoint, every element of A, and in particular s, satisfies φ.

(c) We first argue that in finitely-branching model K, any formula $\mu X.\varphi$ with φ quantifier-free is equivalent to $\omega X.\varphi$. This follows by Homework 4, Exercise 4(a) from the fact that any set operator $A \mapsto \varphi[X/A]$ defined by a quantifier-free formula with one free variable X is continuous in such a model. This can be shown by induction on the structure of φ, the only nontrivial cases being the operators $\wedge$ and $\texttt{[ ]}$.

For $\texttt{[ ]}$, we must show that if $\mathcal{C}$ is a chain of sets of states of K, then

$$\texttt{[}a^K\texttt{]}\bigcup_{A\in\mathcal{C}} A = \bigcup_{A\in\mathcal{C}} \texttt{[}a^K\texttt{]}A, \tag{3}$$

where we define

$$\begin{aligned}\texttt{[}a^K\texttt{]}A &\stackrel{\text{def}}{=} \{s \mid N_a(s) \subseteq A\} \\ N_a(s) &\stackrel{\text{def}}{=} \{t \mid (s,t) \in \mathfrak{m}_K(a)\}.\end{aligned}$$

Since K is finitely branching, $N_a(s)$ is finite. If $N_a(s) \subseteq \bigcup_{A\in\mathcal{C}} A$, then there exists an $A \in \mathcal{C}$ such that $N_a(s) \subseteq A$, since $N_a(s)$ is finite and $\mathcal{C}$ is a chain; this gives the forward inclusion of (3). The reverse inclusion follows from the monotonicity of $\texttt{[}a^K\texttt{]}$.

Now suppose for a contradiction that $\mathsf{A}\Diamond\Box\neg p$ is equivalent to a formula $\mu X.\varphi$, where φ is quantifier-free. Since φ defines a continuous operator, $\mu X.\varphi$ is equivalent to $\omega X.\varphi$, which is equivalent to the countable join $\bigvee_{n<\omega} nX.\varphi$. Thus if $s \vDash \mathsf{A}\Diamond\Box\neg p$ then $s \vDash nX.\varphi$ for some n. But $nX.\varphi$ is a quantifier-free formula, and such formulas only depend on finitely many states below the root. Thus we can construct a tree model with root t satisfying $\neg\mathsf{A}\Diamond\Box\neg p = \mathsf{E}\Box\Diamond p$ that agrees with s sufficiently deeply in the tree so that $t \vDash nX.\varphi$ as well. This is a contradiction, since $nX.\varphi \to \mathsf{A}\Diamond\Box\neg p$. The same argument applies to the complement $\mathsf{E}\Box\Diamond p$, so that $\mathsf{A}\Diamond\Box\neg p$ cannot be represented by a formula $\nu X.\varphi$, where φ is quantifier-free. $\Box$

We can actually prove a somewhat stronger statement: $\mathsf{A}\Diamond\Box\neg p$ is not equivalent to any formula of μ/ν alternation depth less than 2. (A formula has *μ/ν alternation depth n* if there exist subformulas $\sigma_1 X_1.\varphi_1, \ldots, \sigma_n X_n.\varphi_n$ such that

- $\sigma_{i+1}X_{i+1}.\varphi_{i+1}$ is a subformula of $\sigma_i X_i.\varphi_i$, $1 \le i \le n-1$,
- $\sigma_i = \mu$ iff $\sigma_{i+1} = \nu$, $1 \le i \le n-1$,

and n is the maximum number for which this is true.)

The proof uses the Baire Category Theorem, which states that in any complete metric space, a countable union of nowhere dense sets cannot cover the whole space. The space of all binary branching tree models over a fixed vocabulary forms a complete metric space, where we define the distance between two tree models to be 2^{-d}, where d is the depth at which the two trees first differ. That is, if $x \in \{0,1\}^*$ such that $s \vDash \langle x \rangle p$ and $t \vDash \langle x \rangle \neg p$ for some atomic formula p, where s and t are the roots of the two trees, and if x is the shortest string for which this is true, then their distance is $2^{-|x|}$. The basic open neighborhoods of this space are described by quantifier-free formulas that completely describe a model down to some finite depth d. A set A is *dense* if it intersects every nonempty open neighborhood. Note that both $\mathsf{A}\Diamond\Box\neg p$ and its complement $\mathsf{E}\Box\Diamond p$ are dense. A set A is *nowhere dense* if every nonempty open set contains a nonempty open subset disjoint from A.

Now suppose $\mathsf{A}\Diamond\Box\neg p$ is equivalent to a μ-formula of quantifier depth 1. As argued above, we can replace any subformula $\mu X.\varphi$ with $\bigvee_{n<\omega} nX.\varphi$. Assuming the formula is in positive form, we can also replace any subformula $\nu X.\varphi$ with $\bigwedge_{n<\omega} \overline{n}X.\varphi$, where

$$\overline{\alpha}X.\varphi \quad \stackrel{\text{def}}{=} \quad \neg\alpha X.\neg\varphi[X/\neg X].$$

Since the formula is of depth 1, no countable join occurs in the scope of a countable meet or vice versa. Thus by continuity, we can move all the countable join operators out front, then move all the countable meet operators out front behind the join operators. We can also combine the countable joins into a single join by taking maxima and the countable meets into a single meet by taking minima, since the quantification is over chains. The resulting formula is of the form

$$\bigvee_{m<\omega} \bigwedge_{n<\omega} \psi_{m,n}, \tag{4}$$

where the $\psi_{m,n}$ are quantifier-free, and this formula is equivalent to $\mathsf{A}\Diamond\Box\neg p$.

We now claim that the sets of models represented by the subformulas

$$\bigwedge_{n<\omega} \psi_{m,n} \tag{5}$$

of (4) are nowhere dense. We need to show that every nonempty open set U contains a nonempty open subset V such that no element of V satisfies (5); equivalently, such that every element of V satisfies

$$\bigvee_{n<\omega} \neg\psi_{m,n}. \tag{6}$$

Let U be a nonempty open set. Since $\mathsf{E}\Box\Diamond p$ is dense, U contains a point s satisfying $\mathsf{E}\Box\Diamond p$. The model s also satisfies (6), since $\mathsf{E}\Box\Diamond p$ is equivalent to the conjunction of (6) over all m. Thus the intersection of U and the open set described by (6) is the desired V.

Exactly the same argument applies to the complement $\mathsf{E}\Box\Diamond p$; we only used the density of $\mathsf{E}\Box\Diamond p$ in the argument above, and similarly we only need the density of $\mathsf{A}\Diamond\Box\neg p$ here. Thus the sets of models represented by $\mathsf{A}\Diamond\Box\neg p$ and $\mathsf{E}\Box\Diamond p$ are both countable unions of nowhere dense sets, therefore so is their union, which is the entire space. But this contradicts the Baire Category Theorem.