Midterm Exam

15-414/614 Bug Catching: Automated Program Verification
Matt Fredrikson André Platzer

October 19, 2017

Name: André Platzer

Andrew ID: aplatzer

Instructions

- This exam is closed-book with one sheet of notes permitted.
- You have 80 minutes to complete the exam.
- There are 5 problems on 6 pages.
- Read each problem carefully before attempting to solve it.
- Do not spend too much time on any one problem.
- Consider if you might want to skip a problem on a first pass and return to it later.

	Max	Score
What Why3 Did Why?	40	
Loop Invariants	50	
Bad Rules	20	
Good Axioms	20	
Estranged Programs	20	
Total:	150	

Please keep in mind that this is a sample solution, *not a model solution. Problems admit multiple correct answers, and the answer the instructor thought of may not necessarily be the best or most elegant.*

1 What Why3 Did Why? (40 points)

Verification tools like Why3 take a correctness statement about a program as input and phrase them in simpler logic. Your job in this question is to provide a sequent calculus proof justifying why this reduction from a DL formula (conclusion) to arithmetic (premise) was correct. Fill in the blanks of the proof to justify correctness. Or else explain why the reduction was unsound.

20 **Task 1**

$$\cfrac{\cfrac{\cfrac{x = a \vdash x + y - y = a}{\qquad\qquad}}{\qquad\qquad}}{x = a \vdash [x := x + y; y := x - y]\, y = a}$$

Solution:

$$\cfrac{\cfrac{\cfrac{x = a \vdash x + y - y = a}{\text{[:=]}\; x = a \vdash [x := x + y][y := x - y]\, x - y = a}}{\text{[:=]}\; x = a \vdash [x := x + y][y := x - y]\, y = a}}{\text{[;]}\; x = a \vdash [x := x + y; y := x - y]\, y = a}$$

20 **Task 2**

$$\cfrac{\cfrac{\cfrac{x \neq 0, x > 0 \vdash 2x + 1 > 0}{\qquad\qquad}}{\qquad\qquad}}{x \neq 0 \vdash [\texttt{if}(x > 0)\, x := 2x + 1]\, x > 0}$$

Solution: Unsound reduction, because the premise is valid but the conclusion is not. The reduction forgot to handle the empty else case, in which case $x > 0$ is not true after the program if $x > 0$ is false initially such that the program has no effect, e.g. when $x = -5$.

2 Loop Invariants (50 points)

Recall the loop invariant proof rule: (while) $\dfrac{\Gamma \vdash J, \Delta \quad J, Q \vdash [\alpha]J \quad J, \neg Q \vdash P}{\Gamma \vdash [\texttt{while}(Q)\,\alpha]P, \Delta}$

In each of the following examples, identify a loop invariant J for which all three premises resulting from applying this loop rule will prove. You do not need to show the proof but should convince yourself that the subgoals are valid.

$\boxed{10}$ **Task 1** $x = 2 \vdash [\texttt{while}(x \leq 10)\,\{x := x + 1\}]x \geq 0$

$J \equiv$ $x \geq 0$

$\boxed{10}$ **Task 2** $x = 2 \vdash [\texttt{while}(x \leq 10)\,\{x := x + 1\}]x = 11$

$J \equiv$ $x \leq 11$

$\boxed{10}$ **Task 3** $x = 2, x = y \vdash [\texttt{while}(x \leq 10)\,\{x := x + y\}]x = 12$

$J \equiv$ $x \leq 12 \land y = 2 \land 2|x$

$\boxed{20}$ **Task 4** $i = 1, \forall j\,(j \geq 0 \rightarrow a(j) > 0) \vdash [\texttt{while}(i < 10)\,\{a(i) := a(i-1) + a(i);\ i := i + 1\}]a(i) \geq 0$

$J \equiv$ $i \geq 1 \land \forall j\,(j \geq 0 \rightarrow a(j) > 0)$

3 Bad Rules (20 points)

Proof rules have to be sound, i.e. if all premises are valid then the conclusion has to be valid. Show that the following proof rules are unsound by giving a counterexample, i.e. an instance of the proof rule for which **all premises are valid but the conclusion is not valid**.

To get you started, here is an example of a proof rule:

$$\text{(R2)}\ \frac{\Gamma, \phi, \psi \vdash \Delta}{\Gamma, \phi \lor \psi \vdash \Delta}$$

R2 is unsound as shown by the following counterexample with valid premises (by arithmetic) but invalid conclusion (e.g. $\omega(x) = 2$ satisfies antecedent but not succedent $x = 0$):

$${\scriptstyle \text{R2}}\frac{x \geq 0, x \leq 0 \vdash x = 0}{x \geq 0 \lor x \leq 0 \vdash x = 0}$$

$\boxed{20}$ **Task 1** (R3) $\dfrac{\Gamma \vdash J \quad J, Q \vdash [\alpha]J \quad \mathbf{\Gamma}, J, \neg Q \vdash P}{\Gamma \vdash [\mathtt{while}(Q)\, \alpha]P}$ with context Γ added to the last premise (**bold**)

Solution: The following sequent calculus proof uses R3 to prove a property that is not true, because the one and only loop body iteration will set x to 1 not 0.

$${\scriptstyle \text{R3}}\cfrac{{\scriptstyle \top\text{R}}\cfrac{*}{x = 0 \vdash \mathit{true}} \quad {\scriptstyle [:=]}\cfrac{{\scriptstyle \top\text{R}}\cfrac{*}{\mathit{true}, x < 1 \vdash \mathit{true}}}{\mathit{true}, x < 1 \vdash [x := x + 1]\mathit{true}} \quad {\scriptstyle \text{id}}\cfrac{*}{\boldsymbol{x = 0}, \mathit{true}, \neg x < 1 \vdash x = 0}}{x = 0 \vdash [\mathtt{while}(x < 1)\, x := x + 1]x = 0}$$

4 Good Axioms (20 points)

Axioms have to be sound, i.e. all their instances valid. Recall that a deterministic program can never reach two different final states from the same initial state.

$\boxed{20}$ **Task 1** Is the following axiom sound for **deterministic** programs? If so use the semantics of dynamic logic to prove soundness or else give a counterexample:

$$\langle\alpha\rangle P \rightarrow [\alpha]P$$

Solution: Let α be a deterministic program, i.e., such that for every initial state ω there is at most one final state ν such that $(\omega, \nu) \in [\![\alpha]\!]$. In order to show $\vDash \langle\alpha\rangle P \rightarrow [\alpha]P$ consider any state ω in which $\omega \models \langle\alpha\rangle P$ and show that $\omega \models [\alpha]P$. By $\omega \models \langle\alpha\rangle P$ there is a state ν such that $(\omega, \nu) \in [\![\alpha]\!]$. Since α is deterministic, there is no other such state. By $\omega \models \langle\alpha\rangle P$ also $\nu \models P$. Since ν is the only final state reachable by α from ω and $\nu \models P$, thus, $\omega \models [\alpha]P$.

5 Estranged Programs (20 points)

Recall that the DL formula $[\alpha]P$ expresses that program α satisfies the partial correctness statement that P holds after all of its runs (if any).

Give an example of a program α for which the following conjunction of DL formulas is valid or explain why no such program exists:

$$[\alpha]\,x = 1 \;\land\; [\alpha]\,x = 2$$

Solution: The following conjunction is true, because its loop never terminates, so every postcondition is vacuously true after it terminates, even contradictory ones like $x = 1$ as well as $x = 2$:

$$[\mathtt{while}(\mathit{true})\,x := x + 1]\,x = 1 \;\land\; [\mathtt{while}(\mathit{true})\,x := x + 1]\,x = 2$$