

ECS 240: Homework Assignment 3

(Due: Thursday, May 22, 2008)

May 8, 2008

(Exercise 1) Two Hoare rule-based proofs

1. Prove using Hoare rules the following property:

$\{x \text{ is even}\} \text{ while } b \text{ do } x := x + 2 \{x \text{ is even}\}$ for any boolean command b

2. Prove using Hoare rules the correctness of Euclid's GCD algorithm:

```
{a > 0 ∧ b > 0}
x := a; y := b
while x ≠ y do
  if x > y then
    x := x - y
  else
    y := y - x
  end if
end while
{gcd(a, b) = x}
```

(Exercise 2) Alternative rules for **while**

1. Consider the following alternative Hoare rule for **while**:

$$\frac{\vdash \{A\} c \{b \Rightarrow A \wedge \neg b \Rightarrow B\}}{\vdash \{b \Rightarrow A \wedge \neg b \Rightarrow B\} \text{ while } b \text{ do } c \{B\}}$$

Show that the system of axioms remains complete if we replace the old rule for **while** with this one. You must show that any derivation that uses the old rule for **while** can be written with this rule instead.

2. Consider the following alternative Hoare rule for **while**

$$\frac{\vdash \{A \wedge b\} c \{A\}}{\vdash \{A\} \text{ while } b \text{ do } c \{A\}}$$

This rule is not complete. Give a counterexample and a short justification.

3. Consider now another Hoare rule for **while**:

$$\frac{\vdash \{A\} c \{A\}}{\vdash \{A\} \text{ while } b \text{ do } c \{A \wedge \neg b\}}$$

This rule is also incomplete. Give a counterexample and a short justification.

(Exercise 3) In the abstract interpretation example with the factorial, you can see that the analysis was rather imprecise. How can you improve the result of this analysis by:

1. Changing the factorial program but not changing the analysis, and
2. Changing the abstract interpretation setup but without changing the factorial program.

Give separate solutions for each of the above ways to address the problem.