Assignment 5: Termination
15-414/15-424 Bug Catching: Automated Program Verification

Due: **11:59pm**, Sunday 10/7/18
Total Points: 30

1. **Find the variant (5 points)** In Homework 3, you developed a loop invariant for the `gcd` program.

$$0 < a \land 0 < b \to [c := a; d := b; \texttt{while}(c \neq d)\,\{\texttt{if}(c > d)\, c := c - d\, \texttt{else}\, d := d - c](c = gcd(a, b))$$

   Now give a variant term that is sufficient to prove the corresponding total correctness formula.

$$0 < a \land 0 < b \to \langle c := a; d := b; \texttt{while}(c \neq d)\,\{\texttt{if}(c > d)\, c := c - d\, \texttt{else}\, d := d - c\rangle(c = gcd(a, b))$$

   For now, you do not need to give a proof, but do concisely explain why your variant term is sufficient. You may refer to your invariant from homework 3 when justifying the variant.

2. **Inductive premise (10 points)** Now prove the inductive premise of the (var) rule for the `gcd` program using your variant from problem 1 and your invariant from Homework 3.

$$J, Q, \varphi = n \vdash \langle \texttt{if}(c > d)\, c := c - d\, \texttt{else}\, d := d - c\rangle(J \land \varphi < n)$$

   You are free to assume in your proof that the inductive premise of the (while) rule for your invariant J has already been proven.

3. **More variants and invariants (5 points)** Consider the following program α, which finds the index of the maximum element of an array a of length n.

```
i := 0;
j := n-1;
while(i ≠ j) {
  if(a(i) ⩽ a(j))
    i := i + 1;
  else
    j := j - 1;
}
```

   Find a loop invariant and variant term sufficient to prove the validity of the formula:

$$0 < n \to \langle\alpha\rangle\,(0 \leqslant i < n \land \forall k.0 \leqslant k < n \to a(k) \leqslant a(i))$$

   You do not need to show a full proof, but justify the correctness of your variant and invariant.

4. **Soundness of $\mathrm{K}_{\langle\cdot\rangle}$ (10 points)** We discussed the modal modus ponens axiom $\mathrm{K}_{\langle\cdot\rangle}$:

$$(\mathrm{K}_{\langle\cdot\rangle})\quad [\alpha](P \to Q) \to (\langle\alpha\rangle P \to \langle\alpha\rangle Q)$$

   We used this to derive the inv2var rule, which is immensely useful as it allows us to use a previously-proved invariant property in our diamond proofs for convergence. Prove the soundness of $\mathrm{K}_{\langle\cdot\rangle}$.