Homework 3 (pen and paper)

Problem 1 - Counterexamples

We call relation $r \subseteq S \times S$ functional if $\forall s, s_1, s_2 \in S$, if $(s, s_1) \in r$ and $(s, s_2) \in r$ then $s_1 = s_2$. For each of the following statements either give a counterexample or prove it ($Q \subset S$):

1. for any r, $wp(r, S \setminus Q) = S \setminus wp(r, Q)$
2. if r is functional, $wp(r, S \setminus Q) = S \setminus wp(r, Q)$
3. for any r, $wp(r, Q) = sp(Q, r^{-1})$
4. if r is functional, $wp(r, Q) = sp(Q, r^{-1})$
5. for any r, $wp(r, Q_1 \cup Q_2) = wp(r, Q_1) \cup wp(r, Q_2)$
6. if r is functional, $wp(r, Q_1 \cup Q_2) = wp(r, Q_1) \cup wp(r, Q_2)$
7. for any r, $wp(r_1 \cup r_2, Q) = wp(r_1, Q) \cup wp(r_2, Q)$
8. $S \neq \emptyset \wedge dom(r) = S \wedge \Delta_S \cap r = \emptyset \rightarrow r \circ r \cap ((S \times S) \setminus r) \neq \emptyset$
   What is the smallest size of the set S for which you can find a counterexample relation r?

Problem 2

Consider the following code fragment:

```
while (x > 0) {
 y = y + x;
 x = x - 3
}
```

Assume that program state contains exactly the two variables, x and y, ranging over unbounded integers

1. Convert the program into guarded commands.
2. Find a formula $F(x, y, x', y')$ describing (precisely) the relationship between initial and final states. Explicitly refer to each rule for constructing formulas that you use. Feel free to refer to relational semantics if needed (e.g. for transitive closure). The final result should be a closed-form formula that is as simple as possible. You can use all valid equations on integers and rules of first-order logic, but explain which rules you use. If some steps in finding the formula need proofs by induction, then carry out such proof.
3. Let $r = \{((x, y), (x', y')) \mid F(x, y, x', y')\}$ be the relation computed for the program in the previous part. Let P be the formula $y == 0$. Find the strongest postcondition formula Q with respect to F, i.e. the formula Q such that the following is a Hoare triple

$$\{(x, y) \mid P\}\ r\ \{(x, y) \mid Q\}$$

4. Find a precondition formula P for the postcondition formula Q: $x < 0$
5. Find a precondition formula P for the postcondition formula Q: $y < 0$
6. Find a precondition formula P for the postcondition formula Q: $x == y$
7. Prove that $r \subseteq s$ where

$$s = \{((x, y), (x', y')) \mid ((y == 0 \land x > 10) \rightarrow y' > 25\}$$

The precondition and postcondition formulas may use mathematical expressions if necessary, but should be as simple as possible.