Clarifications

August 12, 2004

I'm not sure if everybody followed the reasoning I used in class to obtain the relational semantics of a program computing the quotient and remainder of two natural numbers. Hence this note of clarification. To facilitate understanding, I will use notation and terminology discussed in class.
Consider the following program (command) C, where text after "#" is treated as comments:

```
# command C
(
 Q := 0;            # command C0
 while (X >= Y) do # command C1
  (
   X := X - Y;      #   command C10
   Q := Q + 1;      #   command C11
  )
)
```

Assume that the domain of each of X, Y and Q is the set of natural numbers $\mathbf{N}$.
Reasoning intuitively and informally, we expect the relational semantics of C to be something like: $\underline{C} = \{(s, s') \mid (s(X) = s(Y) * s'(Q) + s'(X)) \wedge (0 \leq s'(X) < s(Y)) \wedge (s'(Y) = s(Y))\}$
In other words, we expect the program to terminate if the initial value of Y, i.e. $s(Y)$, is greater than 0, and that of X, i.e. $s(X)$, is at least 0 (which is true in any case since $X \in \mathbf{N}$). On termination, we expect the final value of Q, i.e. $s'(Q)$, to be $s(X)$ div $s(Y)$ (quotient of dividing the initial value of X by the initial value of Y). Similarly, on termination, we expect the final value of X, i.e. $s'(X)$ to be $s(X)$ mod $s(Y)$ (remainder of dividing the initial

value of X by the initial value of Y). The value of Y remains unchanged during the execution of the program.
Given this expected semantics based on our intuitive and informal inspection of the program, we now embark on a formal examination of the relational semantics of C.
By definition, $\underline{C} = \underline{C0} \circ \underline{C1}$.
Since $C0$ is "`Q := 0`", by definition, $\underline{C0} = \{(s, s') \mid s' = s[Q \leftarrow 0]\}$.
Thus, $\underline{C} = \{(s, s'') \mid (s[Q \leftarrow 0], s') \in \underline{C1}\}$. If we look at this equation differently, $\underline{C}$ can be defined by the following two step process:

1. First define $r = \{(s, s'') \mid (s(Q) = 0) \wedge (s, s'') \in \underline{C1}\}$.
2. Then define $\underline{C}$ as $\{(s[Q \leftarrow d], s'') \mid ((s, s'') \in r \wedge d \in \mathbf{N}\}$.

Since the second step above is the easier one, let us focus on the first step for the time being. As defined above, r is clearly $(Q = 0)\rceil\, \underline{C1}$. In other words, we are interested in the relational semantics of $C1$ given that Q has the value 0 in the starting state.
Since $C1$ is "`while (X >= Y) do (C10; C12)`", by definition, $\underline{C1} = lfp\ F(\zeta)$, where $F(\zeta)$ is a function from relations on states to relations on states defined as:

$$F(\zeta) = \delta\lceil (X < Y) \cup ((X \geq Y)\rceil\,(\underline{C10} \circ \underline{C11})) \circ \zeta.$$

Thus, the relation r as defined above is $(Q = 0)\rceil\ lfp\ F(\zeta)$.
It is easy to see from the definition of F that $F(\zeta)$ is a monotonic function in the complete lattice of relations on states. In other words, for two relations ζ_1 and ζ_2 on states, such that $\zeta_1 \subseteq \zeta_2$, we have $F(\zeta_1) \subseteq F(\zeta_2)$.
Thus, underapproximations to r can be obtained by considering the following sequence of relations:

- $(Q = 0)\rceil\, F^0(\phi)$,
- $(Q = 0)\rceil\, F^1(\phi)$,
- $(Q = 0)\rceil\, F^2(\phi)$,

  $\vdots$

It isn't too difficult to see what $\underline{C10} \circ \underline{C11}$ is. Specifically, $\underline{C10} = \{(s, s') \mid s' = s[X \leftarrow s(X) - s(Y)]\}$, and $\underline{C11} = \{(s', s'') \mid s'' = s'[Q \leftarrow s(Q) + 1]\}$.

Therefore, $\underline{C10} \circ \underline{C11} = \{(s, s'') \mid s'' = s[X \leftarrow s(X) - s(Y)][Q \leftarrow s(Q) + 1]\}$.
Let us now try to compute the successive approximations to r.

- $F^0(\phi) = \phi$ by definition, so $(Q = 0)\rceil\, F^0(\phi) = \phi$.
- $F^1(\phi) = F(F^0(\phi)) = F(\phi) = \delta\lceil(X < Y)$.

  In other words, this is $\{(s, s') \mid (s = s') \wedge (0 \leq s(X) < s(Y))\}$. Therefore, $(Q = 0)\rceil\, F^1(\phi) = \{(s, s') \mid (s = s') \wedge (s(Q) = 0) \wedge (0 \leq s(X) < s(Y))\}$.

  Trying to fit this in the form of our desired relational semantics, we find that this can be written as $\{(s, s') \mid (s = s') \wedge (s(Q) = 0) \wedge (s'(Q) = 0) \wedge (s(X) = s(Y) * s'(Q) + s'(X)) \wedge (0 \leq s'(X) < s(Y)) \int (s(Y) = s'(Y))\}$

- $F^2(\phi) = F(F^1(\phi) = (\delta\lceil(X < Y)) \cup ((X \geq Y)\rceil\,(\underline{C10} \circ \underline{C11})) \circ F^1(\phi)$. In other words, this is $F^1(\phi) \cup \{(s, s') \mid (s(X) \geq s(Y)) \wedge (0 \leq s'(X) < s'(Y)) \wedge (s'(X) = s(X) - s(Y)) \wedge (s'(Q) = s(Q) + 1) \wedge (s'(Y) = s(Y))\}$.

  Simplifying, we get $\{(s, s') \mid (s'(Q) \leq s(Q) + 1) \wedge (0 \leq s'(X) < s(Y)) \wedge (s(X) = s(Y) * (s'(Q) - s(Q)) + s'(X)) \wedge (s'(Y) = s(Y))\}$.

  Therefore, $(Q = 0)\rceil\, F^2(\phi) = \{(s, s') \mid (s(Q) = 0) \wedge (s'(Q) \leq 1) \wedge (0 \leq s'(X) < s(Y)) \wedge s(X) = (s(Y) * s'(Q) + s'(X)) \wedge (s'(Y) = s(Y))\}$.

- Let's go one more step and try $F^3(\phi)$. By definition, this is $(\delta\lceil(X < Y)) \cup ((X \geq Y)\rceil\,(\underline{C10} \circ \underline{C11})) \circ F^2(\phi)$. It is not hard to see that this is the same as $F^2(\phi) \cup ((X \geq Y)\rceil\,(\underline{C10} \circ \underline{C11}))^2 \circ F^1(\phi)$.

  The second component of the above union is simply $\{(s, s') \mid (s(X) \geq s(Y)) \wedge (0 \leq s'(X) \leq s'(Y)) \wedge (s'(X) = (s(X) - s(Y)) - s(Y)) \wedge (s'(Q) = (s(Q) + 1) + 1) \wedge (s'(Y) = s(Y))\}$.

  Simplifying, we get the second component as $\{(s, s') \mid (s(X) \geq s(Y)) \wedge (0 \leq s'(X) \leq s'(Y)) \wedge (s(X) = s'(Y) * (s'(Q) - s(Q)) + s'(X)) \wedge (s'(Y) = s(Y)) \wedge (s'(Q) = s(Q) + 2)\}$.

  Taking the union with $F^2(\phi)$, we get $\{(s, s') \mid (0 \leq s'(X) \leq s(Y)) \wedge (s(X) = s'(Y) * (s'(Q) - s(Q)) + s'(X)) \wedge (s'(Y) = s(Y)) \wedge (s'(Q) \leq s(Q) + 2)\}$.

Thus, $(Q = 0)\rceil\, F^3(\phi) = \{(s, s') \mid (s(Q) = 0) \wedge (s'(Q) \leq 2) \wedge (0 \leq s'(X) < s(Y)) \wedge (s(X) = s(Y) * s'(Q) + s'(X)) \int (s'(Y) = s(Y))\}$.

It can be observed that there is a lot of similarity between $F^1(\phi)$, $F^2(\phi)$ and $F^3(\phi)$. Since we are interested in $(Q = 0)\rceil\, lfp\ F(\zeta)$, it is prudent to try to generalize from $F^1(\phi)$ and $F^2(\phi)$ to $F^i(\phi)$ and then use induction to obtain $lfp\ F(\zeta)$.
In order to obtain $F^i(\phi)$, we observe that for values of i in $\{1, 2, 3\}$, we have the following pattern: $F^i(\phi) = \{(s, s') \mid (s'(Q)\, le\, s(Q) + (i - 1)) \wedge (s(X) = s(Y) * (s'(Q) - s(Q)) + s'(X)) \wedge (s'(Y) = s(Y)) \wedge (0 \leq s'(X) < s(Y))\}$.
We now ask the question whether the above pattern for $F^i(\phi)$ holds for all $i \geq 0$. Using induction, it is not hard to show that this is indeed the case. In fact, $F^{i+1}(\phi) = (\delta \lceil (X < Y)) \cup ((X \geq Y)\rceil\, (\underline{C10} \circ \underline{C11})) \circ F^i(\phi)$.
If we apply the induction hypothesis on $F^i(\phi)$ and simplify, we obtain $F^{i+1}(\phi) = \{(s, s') \mid (s'(Q)\, le\, s(Q) + 1 + (i - 1)) \wedge (s(X) - s(Y) = s(Y) * (s'(Q) - (s(Q) + 1)) + s'(X)) \wedge (s'(Y) = s(Y)) \wedge (0 \leq s'(X) < s(Y))\}$.
Thus, our induction hypothesis is true for all i greater than or equal to 1.
Therefore, $lfp\ F(\zeta) = \{(s, s') \mid (s(X) = s(Y) * (s'(Q) - s(Q)) + s'(X)) \wedge (s'(Y) = s(Y)) \wedge (0 \leq s'(X) < s(Y))\}$. Hence, $(Q = 0)\rceil\, lfp\ F(\zeta) = \{(s, s') \mid (s(Q) = 0) \wedge (s(X) = s(Y) * s'(Q) + s'(X)) \wedge (s'(Y) = s(Y)) \wedge (0 \leq s'(X) < s(Y))\}$.
Since r of Eqn 1 is $(Q = 0)\rceil\, lfp\ F(\zeta)$, the above also gives the value of r. From Eqn 2, $\underline{C}$ is now obtained as: $\{(s, s') \mid (s(X) = s(Y) * s'(Q) + s'(X)) \wedge (s'(Y) = s(Y)) \wedge (0 \leq s'(X) < s(Y))\}$.
Amazingly enough (or is it?), this matches our expected relational semantics of the program C. The above process was just to show that using completely rigorous methods, it is possible to obtain relational semantics that matches our intended semantics (thereby, **proving** that the program is partially correct). Of course, as you might have noticed above, the "massaging" of $F^i(\zeta)$ to look similar to what we expect does depend on our expected semantics of the program.