# Proving Progress for Program Sequencing

Notes on UNITY: 16-90

Jayadev Misra*
Department of Computer Sciences
The University of Texas at Austin
Austin, Texas 78712
(512) 471-9547
misra@cs.utexas.edu

7/10/90

## 1 Introduction

We interpret the program $F;G$ in operational terms as follows. Program $F$'s execution is started. If a fixedpoint state of $F$ is reached, the execution of $G$ is started from that state. It simplifies matters, and it does not sacrifice generality, to assume that $G$ has no initialization section. (If $G$ has an initialization section, we may consider $G$ to be $G.init;G.assign$ where $G.init$ is a program that has no initialization section itself, but that simulates the initialization of $G$ through its statements and $G.assign$ has no initialization section but the assign-section of $G$.)

We consider the proof of $p \mapsto q$ in $F;G$. Clearly, if $p \mapsto q$ in $F$ and $p \mapsto q$ in $G$ then $p \mapsto q$ in $F;G$. There is, however, a much stronger rule.

$$\frac{p \mapsto q \vee r \text{ in } F \ , \ r \Rightarrow F.FP \ , \ p \vee r \mapsto q \text{ in } G(F.FP)}{p \mapsto q \text{ in } F;G}$$

Here, $r$ is any predicate, $F.FP$ is the fixedpoint predicate of $F$, $G(F.FP)$ is the program whose initial condition is $F.FP$ and whose assign-seciton is that of $G$.

To see the validity of this rule in operational terms, consider a state satisfying $p$ during the execution of $F;G$. If the given state arises during the execution of $G$ then, from $p \vee r \mapsto q$ in $G(F.FP)$, we have $p \mapsto q$ in $G(F.FP)$ and hence $q$ will hold eventually. If the given state arises during the execution of $F$ then, from $p \mapsto q \vee r$ in $F$, $q$ holds or $r$ holds eventually. In the first case, the proof obligation is met; in the second case, from $r \Rightarrow F.FP$, $G$'s execution will be initiated in a state satisfying $r$; from $r \mapsto q$ in $G(F.FP)$ we conclude that $q$ will be eventually established.

Note: Program $F$ may reach its fixedpoint for some—possibly zero—of the initial states. No assumption is made about the termination of $F$ in the above inference rule. □

Example: Let $F$ :: **assign** $x := 5$ **end** $\{F\}$
$G$ :: **assign** $x := x - 1$ **end** $\{G\}$

*This material is based in part upon work supported by the Texas Advanced Research Program under Grant No. 003658–065 and by the Office of Naval Research Contract N00014-90-J-1640.

It is required to show that
$x > 0 \;\mapsto\; x = 0 \quad \text{in } F;G$

We let $p \;\equiv\; x > 0 \qquad q \;\equiv\; x = 0 \qquad r \;\equiv\; x = 5$

We have $F.FP \;\equiv\; x = 5$

Since $r$ and $F.FP$ are identical, our remaining proof obligations are:
1. $x > 0 \;\mapsto\; x = 0 \;\vee\; x = 5$ in $F$,
2. $x > 0 \;\mapsto\; x = 0$ in $G(F.FP)$

Proof of 1:

| | | | |
|---|---|---|---|
| *true* | *ensures* | $x = 5$ in $F$ | , from the text of $F$ |
| *true* | $\mapsto$ | $x = 5$ in $F$ | , definition of $\mapsto$ |
| $x > 0$ | $\mapsto$ | $x = 0 \;\vee\; x = 5$ in $F$, | strengthening lhs and weakening rhs of the above |

Proof of 2:

| | | | |
|---|---|---|---|
| $x = k$ | *ensures* | $x = k - 1$ in $G(F.FP)$ | , from the text of $G$ |
| $x = k$ | $\mapsto$ | $x = k - 1$ in $G(F.FP)$ | , definition of $\mapsto$ |
| $x > 0 \;\wedge\; x = k$ | $\mapsto$ | $(x > 0 \;\wedge\; x = k - 1) \;\vee\; x = 0$ in $G(F.FP)$ | , strengthening the lhs and rewriting the rhs |
| $x > 0$ | $\mapsto$ | $x = 0$ in $G(F.FP)$ | , induction |

□

The previous example did not exploit the fact that $G$ is started in a state satisfying $F.FP$; i.e, the proof would be valid independent of the value assigned to $x$ in $F$. In the next example we show how the initial state of $G$ is exploited.

Example:
Let $F$ :: **assign** $x \;:=\; 5$ **end** $\{F\}$
$G$ :: **assign** $y \;:=\; x + 1$ **end** $\{G\}$
To show that
$\mathit{true} \;\mapsto\; y = 6$ in $F;G$
We let
$p \;\equiv\; \mathit{true} \qquad q \;\equiv\; y = 6 \qquad r \;\equiv\; x = 5 \qquad F.FP \;\equiv\; x = 5$

Our proof obligations (excluding $r \;\Rightarrow\; F.FP$) are
1. $\mathit{true} \;\mapsto\; x = 6 \;\vee\; x = 5$ in $F$
2. $\mathit{true} \;\mapsto\; y = 6$ in $G(F.FP)$

The first property is easily established (from *true ensures* $x = 5$). The second property requires us to use the fact that $G$ is started with initial conditions $x = 5$; note that it is not possible to prove

$\mathit{true} \;\mapsto\; y = 6 \quad \text{in } G$

The proof of (2) is

| | | | | |
|---|---|---|---|---|
| $x = 5$ | *ensures* | $y = 6$ | in $G(F.FP)$ | , from the text of $G$ |
| $x = 5$ | $\mapsto$ | $y = 6$ | in $G(F.FP)$ | , definition of $\mapsto$ |
| $x = 5$ | invariant | | in $G(F.FP)$ | , definition of invariant and text of $G$ |
| *true* | $\mapsto$ | $y = 6$ | in $G(F.FP)$ | , substitution axiom on the above two |

□

## 2 Some Derived Rules

From the given inference rule for progress, we derive a few rules.

- $$\frac{p \mapsto q \text{ in } F \ , \ p \mapsto q \text{ in } G(F.FP)}{p \mapsto q \text{ in } F; G}$$

Proof: Let $r$ be *false*. □

- $$\frac{p \mapsto q \ \vee \ F.FP \text{ in } F \ , \ p \vee F.FP \mapsto q \text{ in } G(F.FP)}{p \mapsto q \text{ in } F; G}$$

Proof: Let $r$ be $F.FP$. □

- $$\frac{p \textit{ unless } q \text{ in } F \ , \ p \mapsto q \vee F.FP \text{ in } F \ , \ p \mapsto q \text{ in } G(F.FP)}{p \mapsto q \text{ in } F; G}$$

Proof: We show that the hypothesis of the previous rule follows from the hypothesis of the above, where $r \equiv p \wedge F.FP$

Proof of $p \mapsto q \vee r$ in $F$:

| | |
|---|---|
| $p$ *unless* $q$ in $F$ | , given |
| $p \ \mapsto \ q \ \vee \ F.FP$ in $F$ | , given |
| $p \ \mapsto \ [p \ \wedge \ (q \ \vee \ F.FP)] \ \vee \ q$ in $F$ | , PSP on the above two |
| $p \ \mapsto \ (p \ \wedge \ F.FP) \ \vee \ q$ in $F$ | , simplifying the rhs |
| $p \ \mapsto \ q \ \vee \ r$ in $F$ | , $r \ \equiv \ p \ \wedge \ F.FP$ |

Proof of $r \ \Rightarrow \ F.FP$: From the definition of $r$

Proof of $p \ \vee \ r \ \mapsto \ q$ in $G(F.FP)$:

| | |
|---|---|
| $p \ \mapsto \ q$ in $G(F.FP)$ | , given |
| $p \ \vee \ r \ \mapsto \ q$ in $G(F.FP)$ | , $p \ \vee \ r \equiv p$ |

□

- $$\frac{p \mapsto r \text{ in } F \ , \ r \Rightarrow F.FP \ , \ \neg p \text{ invariant in } G(F.FP) \ , \ r \mapsto q \text{ in } G(F.FP)}{p \mapsto q \text{ in } F; G}$$

Proof: We derive the hypothesis of the main inference rule from the hypothesis of the above.

| | |
|---|---|
| $p \ \mapsto \ q \ \vee \ r$ in $F$ | , from $p \mapsto r$ in $F$ |
| $r \ \Rightarrow \ F.FP$ | , given |
| $p \ \vee \ r \ \mapsto \ q$ in $G(F.FP)$ | , $p \ \equiv \ false$ using the substitution axiom |

□

The next rule shows that if $F$ is nonterminating and $p \ \mapsto \ q$ in $F$ then $p \ \mapsto \ q$ in $F; G$.

- $$\frac{p \ \mapsto \ q \text{ in } F \ , \ \neg F.FP}{p \ \mapsto \ q \text{ in } F; G}$$

Proof: The program $G(F.FP)$ starts with initial condition *false*. As shown in [1], every property is provable in $G(false)$. Thus, with $r \ \equiv \ false$,

| | |
|---|---|
| $p \mapsto q \vee r$ in $F$ | , from $p \mapsto q$ in $F$ |
| $r \Rightarrow F.FP$ | , $\neg r$ and $\neg F.FP$ |
| $p \vee r \mapsto q$ in $G(F.FP)$ | , trivially |
| Hence $p \mapsto q$ in $F;G$ | |

**Acknowledgment:** This note has been influenced by a talk of Jan van de Snepscheut at The University of Texas, Austin, on May 11, 1990.

# 3 References

1. "Soundness of the Substitution Axiom," J. Misra, *Notes on UNITY: 14–90*, Austin, Texas, March 2, 1990.