A Program-Composition Theorem Involving Fixed-Point

Notes on UNITY: 28–91

(This note subsumes UNITY–03)

Jayadev Misra*

Department of Computer Sciences

The University of Texas at Austin

Austin, Texas 78712

(512) 471-9547

misra@cs.utexas.edu

12/19/91

Theorem: $$\frac{p \ \circ \ q \quad \text{in } G}{p \ \circ \ (q \ \vee \ \neg F.FP) \quad \text{in } F \ [\!]\ G}$$

where $\circ$ is any UNITY operator (*unless* , *ensures* or *leads-to*) and $F.FP$ is the fixed-point predicate of F.

The theorem is proven separately for each operator in the following lemmas.

Lemma 1: $$\frac{p \ \textit{unless} \ q \quad \text{in } G}{p \ \textit{unless} \ (q \ \vee \ \neg F.FP) \quad \text{in } F \ [\!]\ G}$$

Proof:

$p \wedge F.FP$ stable in F	, stability at fixed point
$p \wedge \neg F.FP$ *unless* $\neg F.FP$ in F	, implication
p *unless* $\neg F.FP$ in F	, simple disjunction
p *unless* q in G	, given
p *unless* $q \vee \neg F.FP$ in $F \ [\!]\ G$	, union theorem

□

Lemma 2: $$\frac{p \ \textit{ensures} \ q \quad \text{in } G}{p \ \textit{ensures} \ (q \ \vee \ \neg F.FP) \quad \text{in } F \ [\!]\ G}$$

Proof:

p *unless* $\neg F.FP$ in F	, as in the above proof
p *ensures* q in G	, given
p *ensures* $q \vee \neg F.FP$ in $F \ [\!]\ G$	, weakening rhs and using the union theorem

*This material is based in part upon work supported by the Texas Advanced Research Program under Grant No. 003658–065, by the Office of Naval Research Contract N00014-90-J-1640 and by the National Science Foundation Award CCR–9111912.

Lemma 3: $$\frac{p \;\mapsto\; q \quad \text{in } G}{p \;\mapsto\; (q \;\vee\; \neg F.FP) \quad \text{in } F \,[\!]\, G}$$

Proof: The proof is by structural induction on $p \;\mapsto\; q$ in G.

- p *ensures* q in G : follows from Lemma 2
- $p \mapsto r$ in G, $r \mapsto q$ in G:
  $p \mapsto r \vee \neg F.FP$ in $F \,[\!]\, G$, induction hypothesis
  $r \mapsto q \vee \neg F.FP$ in $F \,[\!]\, G$, induction hypothesis
  $p \mapsto q \vee \neg F.FP$ in $F \,[\!]\, G$, cancellation
- $p.i \mapsto q$ in G where $p = (\exists\, i \;::\; p.i)$:
  $p.i \mapsto q \vee \neg F.FP$ in $F \,[\!]\, G$, induction hypothesis
  $(\exists\, i \;::\; p.i) \mapsto q \vee \neg F.FP$ in $F \,[\!]\, G$, disjunction □

Corollaries

1.

$$\frac{p \;\circ\; \neg F.FP \quad \text{in } G}{p \;\circ\; \neg F.FP \quad \text{in } F \,[\!]\, G}$$

2.

$$\frac{\begin{array}{c} p \;\circ\; q \quad \text{in } G \\ r \;\Rightarrow\; F.FP \end{array}}{p \;\circ\; q \;\vee\; \neg r \quad \text{in } F \,[\!]\, G}$$

Proof:

$p \circ q \vee \neg F.FP$ in $F \,[\!]\, G$, from the theorem
$p \circ q \vee \neg r$ in $F \,[\!]\, G$, weakening the rhs: $\neg F.FP \Rightarrow \neg r$

3.

$$\frac{\begin{array}{c} p \;\circ\; q \quad \text{in } G \\ \neg q \;\Rightarrow\; F.FP \end{array}}{p \;\circ\; q \quad \text{in } F \,[\!]\, G}$$

Proof: Replace r by $\neg q$ in the above corollary.

4. {used in UNITY–19, with $\mapsto$ in place of $\circ$}

$$\frac{\begin{array}{c} p \;\circ\; q \quad \text{in } G \\ r \;\Rightarrow\; F.FP \\ r \textit{ unless } b \quad \text{in } G \end{array}}{(p \;\wedge\; r) \;\circ\; (q \;\wedge\; r) \;\vee\; b \quad \text{in } F \,[\!]\, G}$$

Proof:

	$r \wedge F.FP$ stable in F	, stability at fixed point
	r stable in F	, $r \Rightarrow F.FP$
(4.1)	r *unless* b in $F \,[\!]\, G$	, union theorem: r *unless* b in G
	$p \circ q$ in G	, given
	$p \circ q \vee \neg r$ in $F \,[\!]\, G$	, Corollary 2 with $r \Rightarrow F.FP$
	$p \wedge r \circ (q \wedge r) \vee b$ in $F \,[\!]\, G$	, conjoin (4.1) to the above. For *unless* and *ensures* , apply conjunction rule and for $\mapsto$, PSP

5. {used in UNITY–03; replace b by *false* in Corollary (4)}

$$\frac{\begin{array}{c} p \;\circ\; q \quad \text{in } G \\ r \;\Rightarrow\; F.FP \\ r \text{ stable in } G \end{array}}{(p \,\wedge\, r) \;\circ\; (q \,\wedge\, r) \quad \text{in } F \;[\!]\; G}$$