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:

\[ p \circ q \text{ in } G \]

\[ p \circ (q \lor \neg F.FP) \text{ in } F \parallel G \]

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:

\[ p \text{ unless } q \text{ in } G \]

\[ p \text{ unless } (q \lor \neg F.FP) \text{ in } F \parallel G \]

Proof:

\[ p \land F.FP \text{ stable in } F \]

, stability at fixed point

\[ p \land \neg F.FP \text{ unless } \neg F.FP \text{ in } F \]

, implication

\[ p \text{ unless } F.FP \text{ in } F \]

, simple disjunction

\[ p \text{ unless } q \text{ in } G \]

, given

\[ p \text{ unless } q \lor \neg F.FP \text{ in } F \parallel G \]

, union theorem

Lemma 2:

\[ p \text{ ensures } q \text{ in } G \]

\[ p \text{ ensures } (q \lor \neg F.FP) \text{ in } F \parallel G \]

Proof:

\[ p \text{ unless } \neg F.FP \text{ in } F \]

, as in the above proof

\[ p \text{ ensures } q \text{ in } G \]

, given

\[ p \text{ ensures } q \lor \neg F.FP \text{ in } F \parallel G \]

, 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: \[ p \rightarrow q \text{ in } G \]
\[ p \rightarrow (q \lor \neg F.FP) \text{ in } F \parallel G \]

Proof: The proof is by structural induction on \( p \rightarrow q \text{ in } G \).

- \( p \text{ ensures } q \text{ in } G \): follows from Lemma 2
- \( p \rightarrow r \text{ in } G, r \rightarrow q \text{ in } G \):
  \[ p \rightarrow r \lor \neg F.FP \text{ in } F \parallel G \text{, induction hypothesis} \]
  \[ r \rightarrow q \lor \neg F.FP \text{ in } F \parallel G \text{, induction hypothesis} \]
  \[ p \rightarrow q \lor \neg F.FP \text{ in } F \parallel G \text{, cancellation} \]
- \( p.i \rightarrow q \text{ in } G \) where \( p = (\exists i :: p.i) \):
  \[ p.i \rightarrow q \lor \neg F.FP \text{ in } F \parallel G \text{, induction hypothesis} \]
  \[ (\exists i :: p.i) \rightarrow q \lor \neg F.FP \text{ in } F \parallel G \text{, disjunction} \]

\[ \square \]

Corollaries
1. \[ p \circ \neg F.FP \text{ in } G \]
   \[ p \circ F.FP \text{ in } F \parallel G \]

2. \[ p \circ q \text{ in } G \]
   \[ r \Rightarrow F.FP \]
   \[ p \circ q \lor \neg r \text{ in } F \parallel G \]

Proof:
   \[ p \circ q \lor \neg F.FP \text{ in } F \parallel G \text{, from the theorem} \]
   \[ p \circ q \lor \neg r \text{ in } F \parallel G \text{, weakening the rhs: } \neg F.FP \Rightarrow \neg r \]

3. \[ p \circ q \text{ in } G \]
   \[ \neg q \Rightarrow F.FP \]
   \[ p \circ q \text{ in } F \parallel G \]

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

4. \{used in UNITY–19, with \( \Rightarrow \) in place of \( \circ \)}
   \[ p \circ q \text{ in } G \]
   \[ r \Rightarrow F.FP \]
   \[ r \text{ unless } b \text{ in } G \]
   \[ (p \land r) \circ (q \land r) \lor b \text{ in } F \parallel G \]

Proof:
   \[ r \land F.FP \text{ stable in } F \text{, stability at fixed point} \]
   \[ r \text{ stable in } F \text{, } r \Rightarrow F.FP \]
   \[ (4.1) \text{ r unless } b \text{ in } F \parallel G \text{, union theorem: } r \text{ unless } b \text{ in } G \]
   \[ p \circ q \text{ in } G \text{, given} \]
   \[ p \circ q \lor \neg r \text{ in } F \parallel G \text{, Corollary 2 with } r \Rightarrow F.FP \]
   \[ p \land r \circ (q \land r) \lor b \text{ in } F \parallel G \text{, conjoin (4.1) to the above.} \]

For \textit{unless} and \textit{ensures}, apply conjunction rule
and for \( \Rightarrow \), PSP

2
5. {used in UNITY-03; replace $b$ by $false$ in Corollary (4)}

\[
p \circ q \quad \text{in } G
\]
\[
r \Rightarrow F.FP
\]
\[
r \text{ stable in } G
\]

\[
(p \land r) \circ (q \land r) \quad \text{in } F \parallel G
\]