Leads-to and Program Union

Notes on UNITY: 06-89

Ambuj K. Singh*
Department of Computer Sciences
The University of Texas at Austin
Austin, Texas 78712
(512) 471-9547
ambujsin@cs.utexas.edu

6/20/89

Composition of progress properties has so far been defined for ensures [1]. Here, conditions are developed for composition of $\mapsto$.

Let F, G be two programs that read/write variables x and let p, q, r, b be any predicates.

Theorem 0:

$$\frac{p \;\mapsto\; q \text{ in } F \qquad r \;\wedge\; x = k \;\; \textit{unless} \;\; b \text{ in } G}{p \;\wedge\; r \;\mapsto\; q \;\vee\; \neg r \;\vee\; b \text{ in } F \;[\!]\; G}$$

where k is a free variable.

First, we prove the following lemma.

Lemma:

$$\frac{p \;\textit{ensures}\; q \text{ in } F \qquad r \;\wedge\; x = k \;\textit{unless}\; b \text{ in } G}{p \;\wedge\; r \;\textit{ensures}\; q \;\vee\; \neg r \;\vee\; b \text{ in } F \;[\!]\; G}$$

Proof:

p *ensures* q in F	, assumption	
r *unless* $\neg r$ in F	, antireflexivity	
$p \;\wedge\; r$ *ensures* $q \;\vee\; \neg r$ in F	, simple conjunction	
$p \;\wedge\; r$ *ensures* $q \;\vee\; \neg r \;\vee\; b$ in F	, consequent weakening	(0)
$p \;\wedge\; x = k$ *unless* $x \neq k$ in G	, G reads/writes x	
$r \;\wedge\; x = k$ *unless* b in G	, assumption	
$p \;\wedge\; r \;\wedge\; x = k$ *unless* b in G	, conjunction	
$p \;\wedge\; r$ *unless* b in G	, disjunction over k	
$p \;\wedge\; r$ *unless* $q \;\vee\; \neg r \;\vee\; b$ in G	, consequent weakening	
$p \;\wedge\; r$ *ensures* $q \;\vee\; \neg r \;\vee\; b$ in $F \;[\!]\; G$	, union theorem with (0)	□

Proof of Theorem: By induction on the proof of $p \;\mapsto\; q$ in F.

*This work was partially supported by ONR Contracts N00014-87-K-0510 and N00014-86-0763.

Base case: p *ensures* q in F

$r \ \wedge \ x = k$ *unless* $x \neq k$ in G	, assumption
$p \ \wedge \ r$ *ensures* $q \ \vee \ \neg r \ \vee \ b$ in $F \ [\!] \ G$	, Lemma
$p \ \wedge \ r \ \mapsto \ q \ \vee \ \neg r \ \vee \ b$ in $F \ [\!] \ G$	, definition of $\mapsto$

Induction step:

- $p \ \mapsto \ c$ in F, c *ensures* q in F

$p \ \mapsto \ c$ in F	, assumption
$r \ \wedge \ x = k$ *unless* b in G	, assumption
$p \ \wedge \ r \ \mapsto \ c \ \vee \ \neg r \ \vee \ b$ in $F \ [\!] \ G$	, induction hypothesis
$p \ \wedge \ r \ \mapsto \ (c \ \wedge \ r) \ \vee \ \neg r \ \vee \ b$ in $F \ [\!] \ G$	, predicate calculus (1)
c *ensures* q in F	, assumption
$r \ \wedge \ x = k$ *unless* b in G	, assumption
$c \ \wedge \ r$ *ensures* $q \ \vee \ \neg r \ \vee \ b$ in $F \ [\!] \ G$	, Lemma and above two
$p \ \wedge \ r \ \mapsto \ q \ \vee \ \neg r \ \vee \ b$ in $F [\!] \ G$	, transitivity with (1)

- $p \ \equiv \ \langle \exists \ i \ :: \ p.i \rangle$ and $p.i \ \mapsto \ q$ in F, for all i

$p.i \ \mapsto \ q$ in F	, assumption
$r \ \wedge \ x = k$ *unless* b in G	, assumption
$p.i \ \wedge \ r \ \mapsto \ q \ \vee \ \neg r \ \vee \ b$ in $F \ [\!] \ G$	, induction hypothesis
$p \ \wedge \ r \ \mapsto \ q \ \vee \ \neg r \ \vee \ b$ in $F \ [\!] \ G$	, disjunction over i. □

Corollary:

$$\frac{p \text{ } \textit{until} \text{ } q \text{ in } F \qquad p \ \wedge \ x = k \text{ } \textit{unless} \text{ } q \text{ in } G}{p \ \mapsto \ q \text{ in } F \ [\!] \ G}$$

where p *until* q is defined to be p *unless* $q \ \wedge \ p \ \mapsto \ q$.

Proof:

$p \ \mapsto \ q$ in F	, assumption
$p \ \wedge \ x = k$ *unless* q in G	, assumption
$p \ \mapsto \ q \ \vee \ \neg p$ in $F \ [\!] \ G$	, Theorem 0 and above two (2)
$p \ \wedge \ x = k$ *unless* q in G	, assumption
p *unless* q in G	, disjunction over k
p *unless* q in F	, assumption
p *unless* q in $F \ [\!] \ G$	, union theorem
$p \ \mapsto \ q$ in $F \ [\!] \ G$	, PSP theorem with (2) □

Corollary: (The following result was discovered independently by Jay Misra [2].)

$$\frac{p \ \mapsto \ q \text{ in } F}{p \ \wedge \ x = m \ \mapsto \ q \ \vee \ x \neq m \text{ in } F \ [\!] \ G}$$

where m is free.

Proof:

$x = m$ *unless* $x \neq m$ in G	, antireflexivity
$x = m \ \wedge \ m = k$ *unless* $x \neq m$ in G	, k, m are free
$x = m \ \wedge \ x = k$ *unless* $x \neq m$ in G	, predicate calculus
$p \ \mapsto \ q$ in F	, assumption
$p \ \wedge \ x = m$ *unless* $q \ \vee \ x \neq m$ in $F \ [\!] \ G$	, Theorem 0. □

Theorem 1:

$$\frac{\begin{array}{c} p\ R\ q \text{ in } F \\ r\ \wedge\ x = k\ \textit{unless}\ b \text{ in } G \end{array}}{(p\ \wedge\ r)\ \ R\ \ (q\ \vee\ \neg r\ \vee\ b) \text{ in } F \parallel G}$$

where R denotes one of *unless*, *ensures*, or $\mapsto$ and programs F, G read/write variables x.

Proof: By considering the three possibilities for r separately.

- If R is *ensures* then the proof follows from the lemma to Theorem 0.
- If R is $\mapsto$ then the proof follows from Theorem 0.
- If R is *unless* then the proof is as follows.

$r\ \wedge\ x = k\ \textit{unless}\ b$ in G	, given
$p\ \wedge\ x = k\ \textit{unless}\ x \neq k$ in G	, G reads/writes x.
$p\ \wedge\ r\ \wedge\ x = k\ \textit{unless}\ b$ in G	, conjunction
$p\ \wedge\ r\ \textit{unless}\ b$ in G	, disjunction over k
$p\ \wedge\ r\ \textit{unless}\ q\ \vee\ \neg r\ \vee\ b$ in G	, consequent weakening (3)
$p\ \textit{unless}\ q$ in F	, given
$r\ \textit{unless}\ \neg r$ in F	, antireflexivity
$p\ \wedge\ r\ \textit{unless}\ q\ \vee\ \neg r$ in F	, simple conjunction
$p\ \wedge\ r\ \textit{unless}\ q\ \vee\ \neg r\ \vee\ b$ in F	, consequent weakening
$p\ \wedge\ r\ \textit{unless}\ q\ \vee\ \neg r\ \vee\ b$ in $F \parallel G$	, union theorem with (3) □

Theorem 2:

$$\frac{\begin{array}{c} p\ \mapsto\ q \text{ in } F \\ r\ \Rightarrow\ G.FP \end{array}}{p\ \mapsto\ q\ \vee\ \neg r \text{ in } F \parallel G}$$

Proof: Let x be the set of variables read and written by F, G and let $G.FP$ denote the fixed point of G.

$G.FP\ \wedge\ r\ \wedge\ x = k\ \textit{unless}\ \textit{false}$ in G	, stability at fixed point.
$r\ \wedge\ x = k\ \textit{unless}\ \textit{false}$ in G	, $r\ \Rightarrow\ G.FP$
$p\ \mapsto\ q$ in F	, assumption
$p\ \wedge\ r\ \mapsto\ q\ \vee\ \neg r$ in $F \parallel G$	, Theorem 0 and above two
$p\ \wedge\ \neg r\ \mapsto\ q\ \vee\ \neg r$ in $F \parallel G$	, $p\ \wedge\ \neg r\ \Rightarrow\ q\ \vee\ \neg r$ by predicate calculus
$p\ \mapsto\ q\ \vee\ \neg r$ in $F \parallel G$	, disjunction □

Corollary: (from [4])

$$\frac{\begin{array}{c} p\ \mapsto\ q \text{ in } F \\ r\ \Rightarrow\ G.FP \\ r \text{ is stable in } F \end{array}}{p\ \wedge\ r\ \mapsto\ q\ \wedge\ r \text{ in } F \parallel G}$$

Proof:

$p\ \mapsto\ q$ in F	, assumption
$r\ \Rightarrow\ G.FP$	, assumption
$p\ \mapsto\ q\ \vee\ \neg r$ in $F \parallel G$	, above theorem (4)

$G.FP \ \wedge \ r$ *unless false* in G	, stability at fixed point
r *unless false* in G	, $r \ \Rightarrow \ G.FP$
r *unless false* in F	, assumption
r *unless false* in $F \ [\!] \ G$	, union theorem
$p \ \wedge \ r \ \mapsto \ q \ \wedge \ r$ in $F \ [\!] \ G$	, PSP theorem with (4) $\Box$

References

1. K. Mani Chandy and Jayadev Misra, *Parallel Program Design: A Foundation*, Addison-Wesley, 1988.

2. Jay Misra, personal communication

3. Jay Misra, "General Conjunction and Disjunction Rules for *unless*," *Notes on UNITY: 01-88*, The University of Texas, Austin, Texas, September 1988.

4. Jay Misra, "A Composition Theorem About Fixed Points," *Notes on UNITY: 03-88*, The University of Texas, Austin, Texas, September 1988.