Union Theorem over Progress Properties: Lifting Rule

Jayadev Misra

December 18, 2015

1 Lifting Rule

A rule that allows deriving a progress property in a union of components, given that the property holds in one of the components, is given in Misra [**?**] A simpler rule is given here from which the previous rule can be derived.

Below, f and g are components, and x a tuple of some accessible variables of f that includes all variables that f shares with g. That is, g does not affect f if it preserves the value of x. In the rule below, X is a free variable, therefore universally quantified.

$$\textbf{L} \quad \frac{\begin{array}{c} p \mapsto q \text{ in } f \\ r \wedge x = X \ \textbf{co} \ x = X \vee \neg r \text{ in } g \end{array}}{p \mapsto q \vee \neg r \text{ in } f \ [] \ g}$$

Note: Predicates p and q are over the accessible variables of f since $p \mapsto q$ is a property of f; any local variable of g named in p or q is a constant. Similarly, r is over the accessible variables of g.

Proof of (L) is by induction on the structure of $p \mapsto q$ in f.

1.1 Assume p en q in f

We show that p **en** $q \vee \neg r$ in $f \ [] \ g$, and, hence, $p \mapsto q \vee \neg r$ in $f \ [] \ g$.

From p **en** q in f, we deduce (1,2) below. Now, every action of g preserves values of all local variables of f. Further, since x includes all shared variables of f, any action of g that does not modify x preserves the values of all accessible variables of f. In particular, any such action preserves p, as given in (3) below.

$$p \wedge \neg q \ \textbf{co} \ p \vee q \text{ in } f \qquad (1)$$
$$\textbf{transient} \ p \wedge \neg q \text{ in } f \qquad (2)$$
$$p \wedge x = X \ \textbf{co} \ p \vee x \neq X \text{ in } g \qquad (3)$$

To show p **en** $q \vee \neg r$ in $f \ [] \ g$, we need to show

$p \wedge \neg q \wedge r$ **co** $p \vee q \vee \neg r$ in f [] g, and
transient $p \wedge \neg q \wedge r$ in f [] g.

- $p \wedge \neg q \wedge r$ **co** $p \vee q \vee \neg r$ in f [] g:

$p \wedge x = X$ **co** $p \vee x \neq X$ in g	, from (3)
$r \wedge x = X$ **co** $x = X \vee \neg r$ in g	, from antecedent
$p \wedge r \wedge x = X$ **co** $p \vee \neg r$ in g	, conjunction of the above, weaken rhs
$p \wedge r$ **co** $p \vee \neg r$ in g	, disjunction over all X
$p \wedge \neg q \wedge r$ **co** $p \vee q \vee \neg r$ in g	, strengthen lhs and weaken rhs
$p \wedge \neg q \wedge r$ **co** $p \vee q \vee \neg r$ in f	, strengthen lhs and weaken rhs of (1)
$p \wedge \neg q \wedge r$ **co** $p \vee q \vee \neg r$ in f [] g	, union rule

- **transient** $p \wedge \neg q \wedge r$ in f [] g:

transient $p \wedge \neg q$ in f	, from (2)
transient $p \wedge \neg q \wedge r$ in f	, strengthening
transient $p \wedge \neg q \wedge r$ in f [] g	, concurrency

1.2 Inductive proofs

We show that if $p \mapsto q$ in f has been proved by transitivity or the disjunction rule, the result holds.

1. Suppose in f, $p \mapsto q$ has been proved by $p \mapsto s$ and $s \mapsto q$:

$p \mapsto s \vee \neg r$ in f [] g	, inductively, from $p \mapsto s$ in f
$s \mapsto q \vee \neg r$ in f [] g	, inductively, from $s \mapsto q$ in f
$p \mapsto q \vee \neg r$ in f [] g	, cancellation on above two

2. Suppose in f, $p \mapsto q$ has been proved by $p_i \mapsto q$ for all i in I, and $p = (\vee i : i \in I : p_i)$. For any i in I:

$p_i \mapsto q \vee \neg r$ in f [] g	, inductively, from $p_i \mapsto q$ in f
$(\vee i : i \in I : p_i) \mapsto q \vee \neg r$ in f [] g	
	, disjunction rule
$p \mapsto q \vee \neg r$ in f [] g	, $p = (\vee i : i \in I : p_i)$

2 Special Cases

1. $$\frac{\begin{array}{c} p \wedge r \mapsto q \text{ in } f \\ r \wedge x = X \textbf{ co } x = X \vee \neg r \text{ in } g \end{array}}{p \mapsto q \vee \neg r \text{ in } f \;[]\; g}$$

Proof: Replace p by $p \wedge r$ in L to get the hypotheses of this rule, and the conclusion: $p \wedge r \mapsto q \vee \neg r$ in f [] g. Now, $p \wedge \neg r \mapsto \neg r$ in f [] g, by the implication rule. Taking the disjunction of the two *leads-to* properties, $p \mapsto q \vee \neg r$ in f [] g, the required conclusion of the given rule.

2. $$\frac{p \mapsto q \text{ in } f}{p \wedge x = M \mapsto q \vee x \neq M \text{ in } f \ [] \ g}$$

   Proof: Let r be $x = M$. Then $x = M \wedge x = X$ **co** $x = X \vee x \neq M$ in g, because (1) for $X \neq M$, the lhs is *false*, and (2) for $X = M$, the rhs is *true*, so the property holds vacuously in both cases. The result follows from (L).

3. If f has no shared variable,

   $$\frac{p \mapsto q \text{ in } f}{p \mapsto q \text{ in } f \ [] \ g}$$

   Proof: From (2) above.

3 Notes

1. $r \wedge x = m$ **co** $x = m \vee \neg r$ in g is $r \wedge x = m$ **co** $r \Rightarrow x = m$ in g. The converse,
   $r \wedge x = m$ **co** $x = m \Rightarrow r$ in g, is unsound. Because g may change x while keeping r *true*. Then because of changed x, f may not establish q and r may remain true.

2. A seeming generalization of (L), below, is invalid.

   $$\frac{\begin{array}{c} p \mapsto q \text{ in } f \\ r \wedge x = X \ \mathbf{co} \ x = X \vee s \text{ in } g \end{array}}{p \wedge r \mapsto q \vee s \text{ in } f \ [] \ g}$$

   To see that this rule is invalid, consider a state where $p \wedge r$ holds. Let X be the value of x in that state. Let g take a step in this state that establishes $\neg r$ but preserves the value of x. And, a next step by g that establishes $\neg s$ and changes the value of x. Suppose all future steps preserve $\neg r$ and $\neg s$. No guarantee can be given that q will be established.