Another Theorem on Strengthening the Guard

Jayadev Misra

2/27/04

It is well known that all safety properties of a program are preserved if the guard of any of its statements is strengthened. This note develops a result about progress properties. Also, see Notes on UNITY, 19, "More on Strengthening the Guard".

Let F be a program which includes a statement t with guard q. Let G be a program obtained by strengthening the guard of t.

Theorem $\dfrac{p \mapsto r \text{ in } F}{p \mapsto q \vee r \text{ in } G}$

Proof: By structural induction on the proof of $p \mapsto r$ in F.

• p **en** r in F: Then, $p \wedge \neg r$ **co** $p \vee r$ in F, which also holds in G, because all safety properties are preserved by strengthening the guard. Next, from the definition of **en** , there exists some action s in F so that

$\{p \wedge \neg r\}\ s\ \{r\}$

If $s \neq t$ then this assertion holds in G. If $s = t$ then

$\{p \wedge \neg r\}\ t\ \{r\}$

Thus, execution of t in F in any state satisfying $p \wedge \neg r$ causes a state change, i.e., t executes effectively. Since the guard of t is q,

$p \wedge \neg r \ \Rightarrow\ q$, or
$p \ \Rightarrow\ q \vee r$

Therefore, $p \mapsto q \vee r$ in G.

• $p \ \equiv\ p' \vee p''$, where $p' \mapsto r$ in F and $p'' \mapsto r$ in F: Using induction,

$p' \mapsto q \vee r$ in G
$p'' \mapsto q \vee r$ in G. Using disjunction,
$p \mapsto q \vee r$ in G

• $p \mapsto p' \mapsto r$ in F: Using induction,

$p \mapsto q \vee p'$ in G
$p' \mapsto q \vee r$ in G. Using cancellation,
$p \mapsto q \vee r$ in G

Corollary Let q be the guard of a statement in F which is strengthened to obtain program G. Then,

$\dfrac{p \mapsto q \text{ in } F}{p \mapsto q \text{ in } G}$