More on Strengthening the Guard

Notes on UNITY: 19-90

Jayadev Misra[*]
Department of Computer Sciences
The University of Texas at Austin
Austin, Texas 78712
(512) 471-9547
misra@cs.utexas.edu

7/17/90

1 Introduction

It is well known that strengthening a guard of any statement in a program preserves all its safety properties though certain progress properties may be destroyed. (If all guards are strengthened to false, the corresponding statements would never be executed causing serious disruption in progress.) The purpose of this note is to investigate the conditions under which the strengthening of a guard preserves *all* the progress properties. This question was first considered by Ambuj Singh [4]; the condition proposed here is simpler than the ones he proposed. This result is useful during program refinements.

Suppose we have a program $F \, [\!] \, \alpha$ where

α is a statement of the form, A if r.

We strengthen the "guard," r, to s, i.e., we consider β where

β is, A if s and $s \;\Rightarrow\; r$.

We are interested in the conditions under which all safety and progress properties of $F \, [\!] \, \alpha$ also hold in $F \, [\!] \, \beta$.

It is not hard to see that *ensures* properties are preserved only under very stringent restrictions. Therefore, we will only consider *unless* and *leads-to* properties. The *trails* relation, introduced in [3], is of central importance.

Theorem: Suppose s *trails* r in F, i.e.,

$s \;\Rightarrow\; r \;$ in F, $r \;\mapsto\; s \;$ in F, $s \;\; unless \;\; \neg r \;$ in F .

Then,
$p \;\; unless \;\; q \;$ in $F \, [\!] \, \alpha \;\Rightarrow\; p \;\; unless \;\; q \;$ in $F \, [\!] \, \beta$
$p \;\mapsto\; q \;$ in $F \, [\!] \, \alpha \;\Rightarrow\; p \;\mapsto\; q \;$ in $F \, [\!] \, \beta$.

[*] This material is based in part upon work supported by the Texas Advanced Research Program under Grant No. 003658–065 and by the Office of Naval Research Contract N00014-90-J-1640.

Proof: We give the proof, ignoring the substitution axiom. As shown in [2], the proof can be redone if substitution axiom is taken into account. The proof is given in several major steps.

1. p *unless* q in $\alpha \Rightarrow p$ *unless* q in β:
This merely says that strengthening a guard preserves the safety properties.
p *unless* q in α , assume
$\{p \wedge \neg q \wedge r\}\ A\ \{p \vee q\}$, definitions of *unless* and α
$\{p \wedge \neg q \wedge s\}\ A\ \{p \vee q\}$, since $s \Rightarrow r$, $p \wedge \neg q \wedge s \Rightarrow p \wedge \neg q \wedge r$
$\{p \wedge \neg q\}\ A$ if s $\{p \vee q\}$, rewriting
p *unless* q in β , definitions of *unless* and β

2. p *unless* q in $F \parallel \alpha \Rightarrow p$ *unless* q in $F \parallel \beta$:
using the union theorem and (1).

3. $p \mapsto q$ in $F \parallel \alpha \Rightarrow p \mapsto q$ in $F \parallel \beta$
It is sufficient to show that

4. p *ensures* q in $F \parallel \alpha \Rightarrow p \mapsto q$ in $F \parallel \beta$
because given (4), (3) can be established using induction on the structure of the proof of $p \mapsto q$ in $F \parallel \alpha$.

Given p *ensures* q in $F \parallel \alpha$, using the union theorem, we have,
p *ensures* q in $F \wedge p$ *unless* q in α
or, p *unless* q in $F \wedge p$ *ensures* q in α

In the first case:
p *unless* q in β , from p *unless* q in α, using (1)
p *ensures* q in F , given
p *ensures* q in $F \parallel \beta$, union theorem
$p \mapsto q$ in $F \parallel \beta$, definition of $\mapsto$

Therefore, the remaining proof obligation is

5. p *unless* q in $F \wedge p$ *ensures* q in $\alpha \Rightarrow p \mapsto q$ in $F \parallel \beta$
Assume the antecedent of (5). We prove its consequent through a series of steps.

5.1 $p \wedge \neg q \Rightarrow r$:
p *ensures* q in α , assumed
$\{p \wedge \neg q\}$ A if r $\{q\}$, definitions of *ensures* and α
$p \wedge \neg q \wedge \neg r \Rightarrow q$, from the above
$p \wedge \neg q \Rightarrow r$, from the above

5.2 $p \wedge s$ *ensures* q in β:
p *ensures* q in α , assumed
$\{p \wedge \neg q \wedge r\}$ A $\{q\}$, definitions of *ensures* and α
$\{p \wedge \neg q\}$ A $\{q\}$, $p \wedge \neg q \Rightarrow r$ from (5.1)
$\{p \wedge \neg q \wedge s\}$ A if s $\{q\}$, properties of triples
$p \wedge s$ *ensures* q in β , definitions of *ensures* and β

5.3 $p \ \wedge \ s \ \ unless \ \ q \quad \text{in } F$

$p \ \ unless \ \ q$ in F , assumed

$s \ \ unless \ \ \neg r \quad \text{in } F$, given

$p \ \wedge \ s \ \ unless \ \ (p \ \wedge \ \neg r) \ \vee \ q \quad \text{in } F$, conjunction and weakening the rhs

$p \ \wedge \ s \ \ unless \ \ (p \ \wedge \ \neg q \ \wedge \ \neg r) \ \vee \ q \quad \text{in } F$, rewriting the rhs

$p \ \wedge \ s \ \ unless \ \ q \quad \text{in } F$, $p \ \wedge \ \neg q \ \wedge \ \neg r \ \equiv \ \mathit{false}$ from (5.1)

5.4 $p \ \wedge \ \neg q \ \mapsto \ s \quad \text{in } F \ [\!] \ \beta$

We use a slightly general form of the results in [3] to prove this result:

$$\frac{\begin{array}{c} T \ \Rightarrow \ G.FP \ , \ \{G.FP \text{ is the fixedpoint predicate of } G\} \\ T \ \ unless \ \ r \text{ in } H \\ b \ \mapsto \ b' \text{ in } H \end{array}}{T \ \wedge \ b \ \mapsto \ (T \ \wedge \ b') \ \vee \ r \text{ in } G \ [\!] \ H}$$

This general result can be proven in the same manner as the proof in [3]. Now we have,

$\neg s \ \Rightarrow \ \beta.FP$, from the definition of β

$\neg s \ \ unless \ \ s \quad \text{in } F$, antireflexivity of *unless*

$p \ \wedge \ \neg q \ \mapsto \ s \quad \text{in } F$, from $p \ \wedge \ \neg q \ \Rightarrow \ r$ (5.1) and $r \ \mapsto \ s \quad \text{in } F$ (given)

Therefore,

$p \ \wedge \ \neg q \ \wedge \ \neg s \ \mapsto \ s \quad \text{in } F \ [\!] \ \beta$

$p \ \wedge \ \neg q \ \mapsto \ s \quad \text{in } F \ [\!] \ \beta$, disjunction of the above with $p \ \wedge \ \neg q \ \wedge \ s \ \mapsto \ s$

We are now ready to prove the main result: $p \ \mapsto \ q$ in $F \ [\!] \ \beta$.

$p \ \ unless \ \ q \quad \text{in } F \ [\!] \ \alpha$, from p *ensures* $q \quad \text{in } F \ [\!] \ \alpha$

$p \ \ unless \ \ q \quad \text{in } F \ [\!] \ \beta$, using (2)

$p \ \wedge \ \neg q \ \mapsto \ s \quad \text{in } F \ [\!] \ \beta$, from 5.4

$p \ \wedge \ \neg q \ \mapsto \ (p \ \wedge \ s) \ \vee \ q \quad \text{in } F \ [\!] \ \beta$

, PSP on the above two

$p \ \wedge \ s \ \mapsto \ q \quad \text{in } F \ [\!] \ \beta$, union theorem on (5.2, 5.3)

$p \ \wedge \ \neg q \ \mapsto \ q \quad \text{in } F \ [\!] \ \beta$, cancellation on the above two

$p \ \mapsto \ q \quad \text{in } F \ [\!] \ \beta$, disjunction of the above with $p \ \wedge \ q \ \mapsto \ q \quad \text{in } F \ [\!] \ \beta$. □

The theorem given above applies to strengthening the guard of a single statement. The result can be generalized. Let

$G \quad \text{if } r$

denote the program whose every statement is guarded by r.

Theorem: Suppose

s *detects* $r \quad \text{in } F$ (i.e., $s \ \Rightarrow \ r \quad \text{in } F \ , \ r \ \mapsto \ s \quad \text{in } F$)

and $s \ \ unless \ \ \neg r \quad \text{in } F \ [\!] \ G$.

Then every *unless* and *leads-to* of

$F \ [\!] \ (G \text{ if } r)$

is a property of

$F \ [\!] \ (G \text{ if } s)$.

The proof of this theorem is similar to that of the previous one. We note one special case of this theorem. Let $r \equiv true$. Then $s \Rightarrow r$ trivially holds. The other conditions simplify to $true \mapsto s$ in F and s stable in $F \; [\!] \; G$. These are known as conditions for "self-stabilization" to s; see [1].

Corollary: Suppose
$true \;\mapsto\; s$ in F
and, s stable in $F \; [\!] \; G$
Then every *unless* and *leads-to* property of $F \; [\!] \; G$ is a property of $F \; [\!] \; (G$ if $s)$. □

2 References

1. G. M. Brown, M. G. Gouda, C.-L. Wu, "Token Systems that Self-Stabilize," *IEEE Trans. on Computers* **38**:6, 845–852, 1989.

2. J. Misra, "Soundness of the Substitution Axiom," *Notes on UNITY: 14-90*, Austin, Texas, March 1990.

3. J. Misra, "A Specialization of *detects*," *Notes on UNITY: 18-90*, Austin, Texas, July 1990.

4. Ambuj Singh, "On Strengthening the Guard," *Notes on UNITY: 07-89*, Austin, Texas, June 20, 1989.