On Strengthening the Guard

Notes on UNITY: 07-89

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

It is well-known that strengthening the guard (given an assignment statement A if p, we refer to predicate p as its guard) preserves all *unless* properties. Here, conditions are developed under which strengthening of guard preserves $\mapsto$ properties too.

Let F be a program and let $s :: A$ if p be a statement. Let statement $t :: A$ if $p \wedge q$ be obtained by strengthening the guard of statement s. Then, program $F \parallel t$ preserves all *unless* and *leads-to* properties of program $F \parallel s$ if the following two conditions hold in F.

- $p \mapsto q$
- Let x be the set of variables of $F \parallel s$. Then, there exists a non-increasing function g of x that is bounded from below such that

$$g(x) = k \wedge q \text{ unless } \neg p \vee g(x) < k$$

Proof: Let b *unless* c be a property of $F \parallel s$. Because $\{b \wedge \neg c\}\ s\ \{b \vee c\}$ implies $\{b \wedge \neg c\}\ t\ \{b \vee c\}$, b *unless* c is also a property of $F \parallel t$. Thus, $F \parallel t$ preserves all *unless* properties of $F \parallel s$.

Let $b \mapsto c$ be a property of $F \parallel s$. We prove that $b \mapsto c$ in $F \parallel t$ by induction on the proof of $b \mapsto c$ in $F \parallel s$.

Base case: b *ensures* c in $F \parallel s$.

From the definition of *ensures*, b *unless* c in $F \parallel s$ and there exists a statement u in $F \parallel s$ such that $\{b \wedge \neg c\}\ u\ \{c\}$. If $u \in F$ then observe the following.

b *unless* c in $F \parallel s$	, assumption
b *unless* c in $F \parallel t$	, preservation of *unless*
$\{b \wedge \neg c\}\ u\ \{c\}$	, assumption
b *ensures* c in $F \parallel t$	, definition of *ensures* and $u \in F$
$b \mapsto c$ in $F \parallel t$	, definition of $\mapsto$

which is our proof obligation.

Otherwise $u = s$, i.e., $\{b \wedge \neg c\}\ s\ \{c\}$. Therefore,

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

$b \wedge \neg c \Rightarrow p$, and (0)
$\{b \wedge \neg c\}\ A\ \{c\}$ (1)

We prove the following two properties of program $F \parallel t$,

$b \wedge p \wedge g(x) = k \mapsto (b \wedge p \wedge q \wedge g(x) = k) \vee c \vee g(x) < k$, and (2)
$b \wedge p \wedge q \wedge g(x) = k \mapsto c \vee g(x) < k$ (3)

and then observe the following in $F \parallel t$:

$b \wedge \neg c \Rightarrow p$	, (0)
$b \wedge \neg p \Rightarrow c$	, predicate calculus
$b \wedge \neg p \mapsto c$	, property of $\mapsto$
$g(x) = k$ *unless* $g(x) < k$	, g is non-increasing
$b \wedge \neg p \wedge g(x) = k \mapsto c \vee g(x) < k$	, PSP theorem
$b \wedge p \wedge g(x) = k \mapsto c \vee g(x) < k$	, transitivity on (2), (3).
$b \wedge g(x) = k \mapsto c \vee g(x) < k$	, disjunction
$b \mapsto c$	, disjunction over k and g is bounded from below □

Proof of (2):

$p \mapsto q$ in F	, assumption
$\neg(p \wedge q) \Rightarrow t.FP$	, t is A if $p \wedge q$
$p \mapsto q \vee (p \wedge q)$ in $F \parallel t$	, Theorem 2 in [2] and above two
$p \mapsto q$ in $F \parallel t$	, predicate calculus (4)
b *unless* c in $F \parallel s$	, assumption
b *unless* c in $F \parallel t$	, preservation of *unless*
$b \wedge p \mapsto (b \wedge q) \vee c$ in $F \parallel t$	, PSP Theorem with (4)
$b \wedge p \mapsto (b \wedge \neg c \wedge q) \vee c$ in $F \parallel t$	, predicate calculus
$b \wedge p \mapsto (b \wedge \neg c \wedge p \wedge q) \vee c$ in $F \parallel t$	, $b \wedge \neg c \Rightarrow p$ by (0)
$b \wedge p \mapsto (b \wedge p \wedge q) \vee c$ in $F \parallel t$	, predicate calculus
$g(x) = k$ *unless* $g(x) < k$ in $F \parallel t$	, g is non-increasing
$b \wedge p \wedge g(x) = k \mapsto (b \wedge p \wedge q \wedge g(x) = k) \vee c \vee g(x) < k$ in $F \parallel t$	, PSP theorem □

Proof of (3):

$\{b \wedge \neg c\}\ A\ \{c\}$	, (1)
$\{b \wedge \neg c \wedge p \wedge q\}\ t\ \{c\}$	, t is A if $p \wedge q$
$b \wedge p \wedge q$ *ensures* c in t	, definition of *ensures*
$g(x) = k$ *unless* $g(x) < k$ in t	, g is non-increasing
$b \wedge p \wedge q \wedge g(x) = k$ *ensures* $c \vee g(x) < k$ in t	, simple conjunction (5)
p *unless* $\neg p$ in F	, antireflexivity
$q \wedge g(x) = k$ *unless* $\neg p \vee g(x) < k$ in F	, assumption
$p \wedge q \wedge g(x) = k$ *unless* $\neg p \vee g(x) < k$ in F	, simple conjunction
b *unless* c in F	, b *ensures* c by assumption.
$b \wedge p \wedge q \wedge g(x) = k$ *unless* $(b \wedge \neg p) \vee c \vee g(x) < k$ in F	, conjunction
$b \wedge p \wedge q \wedge g(x) = k$ *unless* $c \vee g(x) < k$ in F	, $b \wedge \neg p \Rightarrow c$ by (0)
$b \wedge p \wedge q \wedge g(x) = k$ *ensures* $c \vee g(x) < k$ in $F \parallel t$	, union theorem with (5) □

This concludes the base case.

Induction step:

- $b \mapsto r$ in $F \parallel s$, r *ensures* c in $F \parallel s$.

  $b \mapsto r$ in $F \parallel t$, induction hypothesis
  $r \mapsto c$ in $F \parallel t$, proof similar to base case
  $b \mapsto c$ in $F \parallel t$, transitivity

- $b \equiv \langle \exists\ i\ ::\ b.i \rangle$ and $b.i \mapsto c$ in $F \parallel s$, for all i

  $b.i \mapsto c$ in $F \parallel t$, induction hypothesis
  $\langle \exists\ i\ ::\ b.i \rangle \mapsto c$ in $F \parallel t$, disjunction over i
  $b \mapsto c$ in $F \parallel t$, $b \equiv \langle \exists\ i\ ::\ b.i \rangle$. □

Corollary: Let statement s be A if p, statement t be A if $p \wedge q$, and F be any program. Then program $F \parallel t$ preserves all *unless* and *leads-to* properties of program $F \parallel s$ if the following two conditions hold in F,

- $p \mapsto q$
- q *unless* $\neg p$.

Proof: Define g to be a constant function. Thus, g is non-increasing and bounded from below. Let x be the set of variables of $F \parallel s$. Then,

q *unless* $\neg p$, given
$g(x) = k$ *unless false* , g is a constant function
$q \wedge g(x) = k$ *unless* $\neg p$, simple conjunction
$q \wedge g(x) = k$ *unless* $\neg p \vee g(x) < k$, weakening

Thus, both the conditions of the previous theorem are satisfied; the desired result follows from its application. □

References

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

2. Ambuj K. Singh, "Leads-to and Program Union," *Notes on UNITY: 06-89*, The University of Texas, Austin, Texas, May 1989.