Soundness of the Substitution Axiom

Notes on UNITY: 14-90

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

3/2/90

1 Introduction

To paraphrase Mark Twain, the unsoundness of the substitution axiom has been greatly exaggerated. Last June, Jan van de Snepscheut showed me an example where p *unless* q, in a given program, for some specific p, q, could be proven "*true*" by application of the substitution axiom and "*false*" by appealing to the original definition. Since then proposals have appeared [2] to eliminate the substitution axiom altogether. The confusion stems from our (poor) choice of the symbol "$\equiv$" to stand for logical equivalence of predicates as well as to denote a definition in [1].

The substitution axiom is a labor-saving device. It allows us to shorten many predicates in a long proof. The engineering advantages of including the substitution axiom outweigh—in my opinion—the disadvantages of requiring a stricter discipline of program composition (see Section 7 of this note or Section 7.2.4 of [1]). However, unsoundness of the substitution axiom is certainly not one of the problems.

In this note, I restate the inference rules for *unless*, *ensures*, *leads-to* and the substitution axiom. I show that every proof employing the substitution axiom can be converted to a proof that proves a slightly different property without appealing to the substitution axiom. It can then be shown that for every property there is a proof that appeals to the substitution axiom only in its last step. I show that the set of inference rules is sound.

2 Inference Rules for *unless, ensures, leads-to*

In the following, s, t are statements of some given program F. Program name is omitted in the following.

- $$\frac{\langle \forall\ s \ ::\ \{p \wedge \neg q\}\ \ s\ \ \{p \vee q\}\rangle}{p\ \ unless\ \ q}$$

*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 26-0679-4200.

- $$\frac{p \;\; unless \;\; q \;,\; \langle \exists\, t \;\; :: \;\; \{p \;\wedge\; \neg q\} \;\; t \;\; \{q\}\rangle}{p \;\; ensures \;\; q}$$

- $$\frac{p \;\; ensures \;\; q}{p \;\; \mapsto \;\; q}$$

- $$\frac{p \;\; \mapsto \;\; r \;,\; r \;\; \mapsto \;\; q}{p \;\; \mapsto \;\; q}$$

- $$\frac{\langle \forall\, m \;\; :: \;\; p.m \;\; \mapsto \;\; q\rangle}{\langle \exists\, m \;\; :: \;\; p.m\rangle \;\; \mapsto \;\; q}$$

3 Substitution Axiom

We state the substitution axiom in a form slightly different, though equivalent, to the one in [1]: For a proof of a given program, any invariant of it can be regarded as a theorem. As a consequence, any invariant in a property can be replaced by *true* and *true* can be replaced by any invariant.

Example: Suppose that the following are invariants of a given program: $I \wedge J$, $q \;\Rightarrow\; r$. Also, assume that $p \wedge I \;\; unless \;\; q$ can be deduced from the program text using the inference rules for *unless*. Then, we can deduce $p \wedge J \;\; unless \;\; r$ as follows.

$p \;\wedge\; I \;\; unless \;\; q$	, given
$q \;\Rightarrow\; r$	, substitution axiom: regard $q \;\Rightarrow\; r$ as a theorem
$p \;\wedge\; I \;\; unless \;\; r$	, from the above two by weakening the rhs
$p \;\wedge\; (I \;\wedge\; J) \;\wedge\; I \;\; unless \;\; r$	, substitution axiom: *true* replaced by $I \;\wedge\; J$ in the lhs
$p \;\wedge\; (I \;\wedge\; J) \;\wedge\; J \;\; unless \;\; r$	, rewriting the lhs
$p \;\wedge\; J \;\; unless \;\; r$	, substitution axiom: $(I \;\wedge\; J)$ replaced by *true*

A shorter proof results by observing that since $I \;\wedge\; J$ is a theorem, then so is I and so is J. Hence from

$$p \;\wedge\; I \;\; unless \;\; r$$

We deduce, by removing I (since $I \;\equiv\; true$) from the lhs and adding J (since $J \;\equiv\; true$) to the lhs,

$$p \;\wedge\; J \;\; unless \;\; r$$

Note: Replacing zero or more occurrences of I by *true* or *true* by I in a predicate p gives us a predicate q where

$$p \;\wedge\; I \;\; \equiv \;\; q \;\wedge\; I$$

Conversely, any q that satisfies the above can be obtained from p by such replacements.

4 Normal Forms of Proofs

A property (a property is of the form p *unless* q, p *ensures* q, $p \mapsto q$, p invariant) is *directly provable* if it can be deduced (from the program text and the given inference rules) without appealing to the substitution axiom. Thus, p *unless* q is directly provable if

$$\langle \forall\ s \ ::\ \{p \wedge \neg q\}\ s\ \{p \vee q\} \rangle$$

and invariant J is directly provable if

$$\text{initially } J \quad \text{and,} \quad \langle \forall\ s \ ::\ \{J\}\ s\ \{J\} \rangle$$

Notation: For a property P and predicate J, $P(J)$ denotes the property obtained by replacing each predicate p in P by $p \wedge J$. Clearly, $P(true)$ is P.

In this section we show that for any property P of a given program, there is an invariant I such that $P(I)$ is directly provable. As a corollary we obtain that any property P can be deduced by appealing to the substitution axiom only in the last step of the proof: First, we prove $P(I)$ directly; next we deduce P from $P(I)$ by replacing I by *true*.

The basic idea behind the main result is the following. Consider any proof of a property P. Let I be the conjunction of all the invariants that have been used in connection with the substitution axiom in this proof. We display a direct proof—i.e., a proof without appeal to the substitution axiom—of $P(I)$. (If the proof of P does not appeal to the substitution axiom then I is *true*.) The idea is to transform every property Q in the proof to $Q(I)$.

As an example consider the first proof of Section 3 that uses the invariants $(I \wedge J)$ and $(q \Rightarrow r)$ in using the substitution axiom. We deduced $p \wedge J$ *unless* r in that proof. Below, we show the proof of $p \wedge J \wedge (I \wedge J) \wedge (q \Rightarrow r)$ *unless* $r \wedge (I \wedge J) \wedge (q \Rightarrow r)$.

$p \wedge I \wedge (I \wedge J) \wedge (q \Rightarrow r)$ *unless* $q \wedge (I \wedge J) \wedge (q \Rightarrow r)$
, from $p \wedge I$ *unless* q (we will justify this step later)
$p \wedge I \wedge (I \wedge J) \wedge (q \Rightarrow r)$ *unless* $r \wedge (I \wedge J) \wedge (q \Rightarrow r)$
, weakening the rhs
$p \wedge J \wedge (I \wedge J) \wedge (q \Rightarrow r)$ *unless* $r \wedge (I \wedge J) \wedge (q \Rightarrow r)$
, rewriting the lhs

It is clear that one appeal to the substitution axiom—replacing the invariant $(I \wedge J) \wedge (q \Rightarrow r)$ by *true* in both sides of the above property—establishes

$p \wedge J$ *unless* r

Theorem (Normal Forms of Proofs): For any property P of a given program there is an invariant I such that $P(I)$ is directly provable.

Proof: Consider any proof of P. Let I be the conjunction of all the invariants that have been used in appeals to the substitution axiom.

Lemma: I is directly provable.

Proof: Suppose that the k^{th} appeal to the substitution axiom, $0 \leq k < N$, uses invariant I_k. Note that I_k may not be directly provable because it may have been established by a previous appeal to the substitution axiom. We have

$$I \quad \equiv \quad \langle \wedge\ k\ :\ 0 \leq k < N \quad :: \quad I_k \rangle$$

We show that I is directly provable using induction on N. For $N = 0$, $I \equiv \mathit{true}$, and true is directly provable. Now suppose, inductively, that I is directly provable. If I_N is directly provable then we have:

initially I and , initially I_N
$\langle \forall\ s \quad :: \quad \{I\} \quad s \quad \{I\} \rangle$ and , $\langle \forall\ s \quad :: \quad \{I_N\} \quad s \quad \{I_N\} \rangle$

We deduce

initially $I\ \wedge\ I_N$
$\langle \forall\ s \quad :: \quad \{I\ \wedge\ I_N\} \quad s \quad \{I\ \wedge\ I_N\} \rangle$, from conjunction property of Hoare-triples.

Hence, $I \wedge I_N$ is directly provable.

If I_N is not directly provable then it has been deduced from some invariant $J \wedge I_N$ by appealing to the substitution axiom. Clearly, $I \Rightarrow J \wedge I_N$. So,

$$I\ \wedge\ I_N \quad \equiv \quad I$$

and hence, $I \wedge I_N$ is directly provable. (end of lemma)

A proof of P consists of three kinds of proof steps:

1. application of an inference rule (such as for *unless*, *ensures* or *leads-to*),
2. asserting that $J \equiv \mathit{true}$ by appealing to the substitution axiom, and
3. replacing a predicate p with a predicate q by replacing J by true or vice versa, where J is a theorem.

We consider each of these steps in turn. (Note that every application of a derived rule can be replaced by a sequence of basic steps of the above kind.)

1. Whenever an inference rule is applied to deduce a property, such as p *unless* q from

   $\langle \forall\ s \quad :: \quad \{p\ \wedge\ \neg q\} \quad s \quad \{p\ \vee\ q\} \rangle$,

   by conjoining the pre- and post-conditions using $\langle \forall\ s \quad :: \quad \{I\} \quad s \quad \{I\} \rangle$

   we can deduce

   $\langle \forall\ s \quad :: \quad \{p\ \wedge\ I\ \wedge\ \neg(q\ \wedge\ I)\} \quad s \quad \{(p\ \wedge\ I)\ \vee\ (q\ \wedge\ I)\} \rangle$

   i.e., $p \wedge I$ *unless* $q \wedge I$

   Similarly, we can replace a deduction of p *ensures* q by one for $p \wedge\ I$ *ensures* $q \wedge I$. If $p \mapsto q$ is deduced (by appealing to one of three inference rules for $\mapsto$), we can now derive $p \wedge I\ \mapsto\ q \wedge I$.

2. Any proof step in which J is asserted to be true by appealing to the substitution axiom is deleted.

3. A proof step in which a theorem J is replaced by true or vice versa to obtain a property Q' from Q can be eliminated. This is because, by replacing J by true or vice versa, we obtain a predicate q from p where

   $$p \ \wedge \ J \ \equiv \ q \ \wedge \ J$$

   Now $Q(I)$, $Q'(I)$ are obtained from Q, Q' by replacing predicates p, q by $p \wedge I$ and $q \wedge I$, respectively. Since $I \Rightarrow J$,

   $$\begin{array}{ll} & p \ \wedge \ I \\ \equiv & p \ \wedge \ I \ \wedge \ J \\ \equiv & q \ \wedge \ J \ \wedge \ I \\ \equiv & q \ \wedge \ I \end{array}$$

   Thus all predicates in $Q(I)$, $Q'(I)$ are identical and hence they are identical properties.

The resulting proof is a direct proof of $P(I)$. □

Corollary: Every property of a program has a proof in which the substitution axiom is used only in the last step.

Proof (from the theorem): For a property P, there is a direct proof of $P(I)$, for some directly provable invariant I. Now add a proof step that appeals to the substitution axiom and replaces I by *true*; this proof step establishes P. □

The theorem shows that the substitution axiom is unnecessary as long as we are willing to deal with proofs in which invariants are carried through in each step. Our experience in constructing a large number of proofs convinces us that the substitution axiom provides an elegant short-cut by removing many repetitions of the invariants.

It should be noted that in the proof of the theorem, we merely exploited the stability of an invariant; we did not require that the invariant hold initially. The latter property of the invariant is used in demonstrating the soundness of the proof system, next.

5 Soundness

In a system such as ours—often called a *positive axiom system*, because negation of a property cannot be deduced—soundness amounts to showing that some properties cannot be deduced for a given program; in the literature this is known as *absolute consistency* [3]. We restrict ourselves to programs whose initial conditions are not identically *false*; call such programs *nontrivial*.

Theorem: For any nontrivial program with initial condition ic, one of the following is not deducible.

$$ic \ \ unless \ \ false$$
$$ic \ \ ensures \ \ \neg ic$$

Proof: Suppose we can deduce both of these properties. Then from the corollary of Section 4, there exist invariants I, J such that

$ic \wedge I \ \ unless \ \ false$ and, (1)
$ic \wedge J \ \ ensures \ \ \neg ic \wedge J$ (2)

are directly provable. From (2), there is a statement t in the program such that

$\{ic \wedge J \wedge \neg(\neg ic \wedge J)\} \ t \ \{\neg ic \wedge J\}$
i.e., $\{ic \wedge J\} \ t \ \{\neg ic \wedge J\}$ (3)
From (1),
$\{ic \wedge I\} \ t \ \{ic \wedge I\}$ (4)
Taking conjunction of (3,4)
$\{ic \wedge I \wedge J\} \ t \ \{false\}$ (5)
Since I, J are invariants $ic \Rightarrow I$ and $IC \Rightarrow J$. Hence, from (5)
$\{ic\} \ t \ \{false\}$ (6)

The only predicate ic satisfying (6) is *false* because every statement terminates in a valid state starting from a valid state.

This contradicts our assumption that ic differs from *false*. □

As an aside we note that every property is deducible in a trivial program (whose initial condition is *false*). This is because: *false* is invariant, from initially *false* and $\langle \forall \ s \ :: \{false\} \ s \ \{false\} \rangle$. We will appeal to the substitution axiom with invariant *false* to prove various properties. For instance, $p \ unless \ q$ is proven by

$false \ \ unless \ \ false$	, from *unless* inference rule
$p \wedge false \ \ unless \ \ q \wedge false$	, rewriting
$p \ \ unless \ \ q$	, substitution axiom: *false* replaced by *true*

Similarly $p \ ensures \ q$ can be proven for arbitrary p, q. Then $p \mapsto q$ follows.

6 Proofs of Derived Rules

Consider a derived rule such as for the disjunction of *unless*es (Section 3.6.1 of [1]):

$$\frac{\begin{array}{c} p \ \ unless \ \ q \\ p' \ \ unless \ \ q' \end{array}}{(p \vee p') \ \ unless \ \ (\neg p \wedge q') \vee (\neg p' \wedge q) \vee (q \wedge q')}$$

The proof in [1] assumes that each of the *unless* properties in the hypothesis is directly provable. Thus it seems that the justification given for this derived rule is incomplete; we must consider the situation where some of the properties in the hypothesis—$p \ unless \ q$, $p' \ unless \ q'$—have been deduced by appealing to the substitution axiom. Fortunately, this is unnecessary; the proof given in the book is sufficient. We show this result, in general.

Lemma: If property P is directly provable then so is $P(I)$, for any directly provable invariant I.

Proof: Similar to the proof of the theorem in Section 4.

Note: $[P(I)](J) = P(I \ \wedge \ J)$

Consider the disjunction rule for *unless*es given above. According to the theorem in Section 4, there is a (directly provable) invariant I such that

$p(I) \ \ unless \ \ q(I)$

is directly provable. Similarly for some (directly provable) invariant J

$p'(J) \ \ unless \ \ q'(J)$

is directly provable.

Using the above lemma

$p(I \ \wedge \ J) \ \ unless \ \ q(I \ \wedge \ J)$ and
$p'(I \ \wedge \ J) \ \ unless \ \ q'(I \ \wedge \ J)$

are both directly provable. Therefore using the arguments in [1] we deduce—where $\hat{p}$ is a shorthand for $p(I \wedge J)$—

$\hat{p} \ \wedge \ \hat{p'} \ \ unless \ \ (\neg\hat{p} \ \wedge \ \hat{q'}) \ \vee \ (\neg\hat{p'} \ \wedge \ \hat{q}) \ \vee \ (\hat{q} \ \wedge \ \hat{q'})$

Now applying the substitution axiom with $I \ \wedge \ J$ we deduce

$p \ \wedge \ p' \ \ unless \ \ (\neg p \ \wedge \ q') \ \vee \ (\neg p' \ \wedge \ q) \ \vee \ (q \ \wedge \ q')$

which is the desired result.

In general, if we have a derived rule of the form

$$\frac{F\ (\ldots,\ p\ ,\ \ldots) \quad G\ (\ldots,\ q\ ,\ \ldots)}{H(\ldots,\ p\ ,\ldots,\ q\ ,\ldots)}$$

where p, q are individual predicates, it is sufficient to establish the rule where each of F, G is directly provable. If they are not directly provable there exist directly provable invariants I, J such that $F(\ldots,\ \hat{p}\ ,\ldots)$ and $G(\ldots,\ \hat{q}\ ,\ldots)$ are directly provable—where $\hat{p} = p(I \wedge J)$, etc. Then $H(\ldots,\ \hat{p}\ ,\ldots,\ \hat{q}\ ,\ldots)$ can be established using the previous argument for the derived rule and $H(\ldots,\ p\ ,\ldots,\ q\ ,\ldots)$ can be established by using the substitution axiom with $I \wedge J$.

Some care has to be exercised in proving a rule of the form

$$\frac{p \ \ unless \ \ q\ ,\ q \ \Rightarrow \ r}{p \ \ unless \ \ r}$$

Here $q \Rightarrow r$ may have been proven by appealing to substitution axiom, i.e., $(q \Rightarrow r) \wedge J$ is invariant, for some directly provable invariant J.

Now observe that

$p \ \wedge \ (q \ \Rightarrow \ r) \ \wedge \ I \ \wedge \ J \ \ unless \ \ q \ \wedge \ (q \ \Rightarrow \ r) \ \wedge \ I \ \wedge \ J$

is directly provable, for some directly provable invariant I. Next applying the arguments in [1], we may weaken the consequence to obtain:

$p \ \wedge \ (q \ \Rightarrow \ r) \ \wedge \ I \ \wedge \ J \ \ unless \ \ r$

Then applying the substitution axiom with $(q \Rightarrow r) \wedge I \wedge J$ we obtain

$p \ \ unless \ \ r$

7 Program Composition

One part of the union theorem (Section 7.2.1 of [1]) states

$$p \ \ unless \ \ q \quad \text{in } F \parallel G = p \ \ unless \ \ q \quad \text{in } F \ \wedge \ p \ \ unless \ \ q \quad \text{in } G$$

The restriction, given in Section 7.2.4 of [1], is that any appeal to the substitution axiom made in any of the proofs—in F, G or $F \parallel G$—can only use the invariants of $F \parallel G$; it is not permissible to deduce p *unless* q in F, say, by using an invariant of F to appeal to the substitution axiom.

Clearly, this restriction poses methodological difficulties—in composing programs together we must not only know the properties of each component but also how each one was derived. There are two ways to address this issue:

1. For each property, supply the conjunction of all the invariants used in appealing to the substitution axiom in its proof, or

2. Assume that the set of properties of a component program includes all invariants used with the substitution axiom in proving all other properties in the set.

We are experimenting with both alternatives to determine the one that proves the easiest in practice.

8 References

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

2. Sanders, Beverly A. [1990]. "Eliminating the substitution axiom from UNITY logic," to appear as *ETH Departement Informatik TR 148*, 1990.

3. Hunter, Geoffrey [1971]. *Metalogic: An Introduction to the Metatheory of Standard First Order Logic*, University of California Press, Berkeley and Los Angeles, California, 1971.