A Note on Subgoal Induction

Jayadev Misra
Department of Computer Sciences
University of Texas, Austin 78712
TR - 91

March 1979

ABSTRACT

We define "power" of an induction rule and show that a slight modification to subgoal induction rule increases its power. We give an infinite sequence of induction rules of strictly increasing power.

KEY Words

Program Verification, Induction Rule, Subgoal Induction

1. Introduction

Subgoal induction, introduced by Morris and Wegbreit [2], is an alternative to the inductive assertion method for proving loop programs. Let x denote a vector of variable values. Given a loop of the form while $B(x)$ do $x \leftarrow s(x)$, it is required to show that a certain relation $\Psi(x_0;x_f)$ holds between every initial value x_0 and the corresponding final value x_f. Subgoal induction requires us to prove the following.

SI::

1. $\neg B(x) \Rightarrow \Psi(x;x)$
2. $B(x) \wedge \Psi(s(x),z) \Rightarrow \Psi(x;z)$

We define Ψ and while $B(x)$ do $x \leftarrow s(x)$, to be consistent with respect to SI if (1) and (2) hold. Clearly consistency implies correctness in the conventional sense though the converse is not true.

In this paper, we consider induction rules of the type SI, which for every Ψ and while $B(x)$ do $x \leftarrow s(x)$, provide verification conditions of the form (1) and (2). Given two induction rules Q and R, we can compare their "power" in the following manner. Q is at least as powerful as R if Ψ , while $B(x)$ do $x \leftarrow s(x)$ are consistent with respect to R implies ψ, while $B(x)$ do $x \leftarrow s(x)$ are consistent with respect to Q. Q is more powerful than R if Q is at least as powerful as R and R is not at least as powerful as Q.

One of the attractions of SI is that verification conditions (1), (2) are directly derivable from the given relation Ψ . It is however possible to have SI' with the following verification conditions.

1. $\exists \psi', \psi'(x,z) \Rightarrow \Psi(x,z)$

2. $\neg B(x) \Rightarrow \psi'(x,x)$

3. $B(x) \wedge \psi'(s(x),z) \Rightarrow \psi'(x,z)$

Condition (1) essentially strengthens the relation Ψ to ψ'; conditions (2) and (3) are the usual SI conditions applied to ψ'. For every *while* $B(x)$ *do* $x \leftarrow s(x)$ and Ψ, such a ψ' can be found if the program is correct with respect to Ψ. We disallow such induction rules since (a) the question of power is not interesting and (b) the use of SI' requires the invention of ψ'. Hence we restrict attention to those induction rules in which the verification conditions can be generated directly from the given program and Ψ.

We first show a slight modification of SI which leads to a rule R_0 that is more powerful than SI. We next define an infinite sequence of rules R_i, $i \geq 1$, such that R_i is more powerful than R_{i-1}, $i \geq 1$.

2. A Modification of SI

SI uses universal quantification for z; however it is sufficient to restrict attention to those values of z for which $\neg B(z)$ hold. This leads to rule R_0.

R_o::

1. $\neg B(x) \Rightarrow \Psi(x;x)$

2. $B(x) \wedge \neg B(z) \wedge \Psi(s(x),z) \Rightarrow \Psi(x;z)$

We leave it to the reader to show that if (1) and (2) hold then $\Psi(x_0,x_f)$ hold for every initial value x_0 and the corresponding final value x_f of the loop. It is more interesting that we can establish

that R_0 is more powerful than SI. For construction of this and future proofs we will use the following program P.

P::

while (t nodiv x) do x:=x-1

t is some arbitrary fixed positive integer > 1

x is initially $\geq$ 0

t nodiv x stands for "t does not divide x"

We will use (t div x) to stand for $\neg$(t nodiv x).

Lemma 1

R_0 is more powerful than SI.

Proof

It is obvious that if for some B,S, Ψ, the verification conditions corresponding to SI hold, then the verification conditions corresponding to R_0 hold. Hence R_0 is at least as powerful as SI.

We next show a loop program and a relation Ψ for which verification conditions (1), (2) for SI do not hold, but verification conditions (1) (2) for R_0 hold. Let P be the program given above. Let $\Psi(x;y) \equiv x-y<t$. $\Psi(x;x)$ holds trivially for all x.

Verification condition (2) for SI is: (t nodiv x) $\wedge$ (x-1-z< t) $\Rightarrow$ (x-z< t)

This is seen to be false by choosing x,t such that t>1 and (t nodiv x) and setting z = x-t.

Verification condition (2) for R_0 is :

(t nodiv x) $\wedge$ (t div z) $\wedge$ (x-1-z< t) $\Rightarrow$ (x-z< t)

This holds. Proof is by contradiction. If x-z$\geq$t then since x-1-z< t, x-z=t. (t div z) $\wedge$ (x-z=t) $\Rightarrow$ (t div x) contradicting the premise .

This proves the lemma.

3. An Infinite Sequence of Induction Rules

R_0 was obtained from SI by restricting the values that z can take. We can further restrict z by considering 3 cases: the loop body is executed 0 times, 1 time, more than one time. We thus postulate R_1.

R_1::

1. $\neg B(x) \Rightarrow \Psi(x;x)$

2.1 $B(x) \wedge \neg B(s(x)) \Rightarrow \Psi(x;s(x))$

2.2 $B(x) \wedge B(s(x)) \wedge \neg B(z) \wedge \Psi(s(x);z) \Rightarrow \Psi(x;z)$

In general, we can define R_k, $k \geq 1$, which has one condition corresponding to each of the following k + 2 cases: the loop body is executed 0 times, 1 time .... k times and more than k times. In the following, we use x_i to denote $s^i(x)$.

R_k::

1. $\neg B(x) \Rightarrow \Psi(x;x)$

2.1 $x_1 = s(x_0) \wedge B(x_0) \wedge \neg B(x_1) \Rightarrow \Psi(x_0;x_1)$

2.i $x_1 = s(x_0) \wedge x_2 = s(x_1) \ldots \wedge x_i = s(x_{i-1}) \wedge$

$B(x_0) \wedge B(x_1) \wedge \ldots \wedge B(x_{i-1}) \wedge \neg B(x_i) \Rightarrow \Psi(x_0;x_i)$

2.k $x_1 = s(x_0) \wedge x_2 = s(x_1) \ldots \wedge x_k = s(x_{k-1}) \wedge$

$B(x_0) \wedge B(x_1) \wedge \ldots \wedge B(x_{k-1}) \wedge \neg B(x_k) \Rightarrow \Psi(x_0;x_k)$

2.(k+1) $x_1 = s(x_0) \wedge x_2 = s(x_1) \ldots \wedge x_k = s(x_{k-1}) \wedge$

$B(x_0) \wedge B(x_1) \wedge \ldots \wedge B(x_{k-1}) \wedge B(x_k) \wedge$

$\neg B(z) \wedge \Psi(x_1;z) \wedge \Psi(x_2;z) \ldots \wedge \Psi(x_k;z) \Rightarrow \Psi(x_0;z)$

Again we leave it to the reader to show that if for any B, s, Ψ and $k \geq 0$, the verification conditions corresponding to R_k hold then $\Psi(x_0;x_f)$ hold for the initial and final values of the loop while B(x) do $x \leftarrow s(x)$.

Theorem R_{k+1} is more powerful than R_k for all $k \geq 0$.

Proof

It is clear that R_{k+1} is at least as powerful as R_k. To prove that R_{k+1} is (strictly) more powerful, we use the program P; choose $t > k + 1$ and let

$$\Psi(x;y) \equiv (x-y) \leq t + k$$

We show that P, Ψ cannot be proven using R_k, but they can be proven using R_{k+1}. Note that $s^i(x) = x-i$.

Ψ is reflexive and hence verification condition (1) holds trivially for every R_k. Consider the verification condition (2.i) in R_k.

2.i: $(t \text{ nodiv } x) \wedge (t \text{ nodiv } x - 1) \ldots \wedge (t \text{ nodiv } x-i+1) \wedge (t \text{ div } x-i) \Rightarrow$

$$(x - (x-i) \leq t + k)$$

This condition holds. However the proposition corresponding to $2\cdot(k+1)$ given below, does not hold.

$2\cdot(k+1)$: $(t \text{ nodiv } x) \wedge (t \text{ nodiv } x-1) \ldots \wedge (t \text{ nodiv } x-k) \wedge$

$$(t \text{ div } z) \wedge (x-1-z \leq t+k) \wedge \ldots \wedge (x-k-z \leq t+k) \Rightarrow x-z \leq t+k$$

This proposition is seen to be false by setting $x = t + k + 1$ and $z = 0$.

Next consider R_{k+1}. By similar arguments the conditions 1, 2.1, ... 2.i...$2\cdot(k+1)$ hold. The induction condition $2\cdot(k+2)$ results in the following propostion.

$2\cdot(k+2)$: $(t \text{ nodiv } x) \wedge (t \text{ nodiv } x-1) \wedge \ldots \wedge (t \text{ nodiv } x-k-1) \wedge$

$(t \text{ div } z) \wedge (x-1-z \leq t+k) \ldots \wedge (x-k-z \leq t+k) \Rightarrow x-z \leq t+k$

$2\cdot(k+2)$ can be proven by contradiction. If $x-z > t+k$ and since $x-1-z \leq t+k$, then $x-z = t+k+1$, or $z = x-t-k-1$. $t \text{ div } z \Rightarrow t \text{ div } z+t$. Hence $(t \text{ div } x-k-1)$. This contradicts $(t \text{ nodiv } x-k-1)$ in the premise.

4. Discussion

It is clear that stronger the relation Ψ, easier it is to prove in the sense that a smaller R_i can be used for proving it. In the example P, $x-z<t$ can be proven using R_0 whereas proof of $x-z \leq t+k$ requires the use of R_{k+1}. Obviously the latter relation is derivable from the former. However inventing a stronger relation is similar to the problem of inventing a loop invariant. The strongest possible relation between x_0, x_f can be given by stating x_f as a certain function of x_0, i.e. $x_f = F(x_0)$. Then R_0 is sufficient for the proof and any other relation $\Psi(x_0;x_f)$ can be proven to hold by deducing it from $x_f = F(x_0)$. One of the attractions of subgoal induction is to derive the verification conditions without explicitly constructing F; we believe therefore that the notion of power is important and the rules for small i will be found useful in practice.

References

1. Misra, J., "Some Aspects of the Verification of loop computations," IEEE Trans. on Software Engineering, Vol. SE-4, No. 6, Nov. 1978, 478-486.

2. Morris, J. H., Jr. and Wegbreit, B., "Subgoal Induction," CACM 20, 4, April 1977, 209-222.