stichting
mathematisch
centrum

AFDELING INFORMATICA
(DEPARTMENT OF COMPUTER SCIENCE)

IW 178/81 SEPTEMBER

D. LEHMANN

ANOTHER PROOF FOR THE COMPLETENESS OF A RULE FOR THE FAIR TERMINATION OF GUARDED COMMANDS AND ANOTHER RULE FOR THEIR JUST TERMINATION
(Preliminary version)

Preprint

kruislaan 413 1098 SJ amsterdam

Printed at the Mathematical Centre, 413 Kruislaan, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

1980 Mathematics subject classification: 68B10, 68C01

ACM-Computing Reviews-category: 5.24

Another proof for the completeness of a rule for the fair termination of guarded commands and another rule for their just termination [*)]
(preliminary version)

by

Daniel Lehmann [**)]

ABSTRACT

A proof is given of the completeness of a rule proposed in [GFMR]. The result is an almost immediate consequence of one of the completeness results of [LPS]. Another completeness result of [LPS] suggests a rule for proving just termination of loops. It is different from the rule proposed in [AO]. It is shown to be sound and complete.

KEY WORDS & PHRASES: *proof rules, termination, fairness, guarded commands, completeness, justice*

[*)] This report will be submitted for publication elsewhere.

[**)] This work was done while the author was a summer visitor at the Mathematisch Centrum, Amsterdam.
Author's permanent address: Institute of Mathematics and Computer Science, Hebrew University, Jerusalem 91904, Israel.

1. INTRODUCTION

We consider an iterative guarded command C of the type:

$$* \,[\, \underset{i \in I}{\Box} \; B_i \to C_i \,]$$

where I is a set of indexes, the B_i's are boolean expressions (without side effects) and the C_i's are commands (there is no assumption of fairness for the successive executions of each C_i).
We make the assumption of fairness at the outer level by assuming that if, in the course of executing C we get an infinite number of times at the beginning of the body of the loop with B_i being true, then we will choose the command C_i for execution an infinite number of times.

In [GFMR] the authors proposed the following proof rule for such commands (with a small insignificant change). To prove $< r > C < q >$ (meaning total correctness under the assumption of fairness), find a set W and a well-founded relation (<) on it, a predicate p on States x W and for each $w \in W$ that is not minimal in W, two subsets of I: D_w and S_w satisfying the following conditions:

(1) $I = D_w \cup S_w$ and $D_w \neq \emptyset$ for every $w \in W$, not a minimal element.

(2) For every $w \in W$, not a minimal element, and every $j \in D_w$

$$< p(w) \wedge B_j > \; C_j \; < \exists\, v < w ,\ p(v) >$$

(3) For every $w \in W$, not a minimal element and every $k \in S_w$:

$$< p(w) \wedge B_k > \; C_k \; < \exists\, v \leq w ,\ p(v) >$$

(4) For every $w \in W$ not a minimal element, such that $S_w \neq \emptyset$

$$< p(w) > \; * \,[\, \underset{k \in S_w}{\Box} \; B_k \wedge \neg \underset{j \in D_w}{\vee} B_j \to C_k \,] \; < \text{true} >$$

(5) For every $w \in W$ a minimal element:

$$p(w) \supset \bigwedge_{i \in I} \neg B_i$$

(6) For every $w \in W$

$$p(w) \wedge \neg \bigvee_{i \in I} B_i \supset q$$

(7) $$r \supset \exists v\ p(v)$$

Another rule to the some effect has been proposed in [AO]. In [GFMR], the completeness of the method is proved by use of a delicate analysis of C's computation tree. Another proof will be proposed, based on [LPS].

2. THE PROOF

Suppose that $< r > C < q >$ holds. We have to find a set W, a well-founded relation $<$, a predicate p and sets D_w and S_w satisfying (1)-(7). Our proof is by induction on the size of the set I of indexes. Suppose we have shown completeness for all iterative commands with strictly less guards than $|I|$.

From our assumption we deduce $< r > C$ <true> and $[r]\ C\ [q]$ (the square brackets mean partial correctness). Let us, first draw some conclusions from the second claim. Since the partial correctness theory is independent of the assumption of fairness, we may apply the classical proof rule which is known to be complete (it seems to be a folk theorem, given as Exercise 7.17 in [B]). Therefore there is a predicate a satisfying:

(a) $$r \supset a$$

(b) For every $i \in I$ $\quad [a \wedge B_i]\ C_i\ [a]$

(c) $$a \wedge \neg \bigvee_{i \in I} B_i \supset q$$

We may also assume that every state satisfying a is reachable (during an execution of C) from some state satisfying r.

Let us now come back to the assertion <r> C <true> . Let A be the set of states $s \in$ States satisfying r. For $i \in I$, define $f_i \subset$ States x States by:

$(s,t) \in f_i$ iff s satisfies B_i and C_i may lead from s to t.
Now with the notations of [LPS] let us consider the concurrent system:
$P = <\text{States}, \{f_i\}_{i \in I}, A>$. There is a one-to-one correspondence between fair computations of P and fair executions of C.
Therefore P fairly terminates and also impartially terminates. By the completeness of method M for proving impartial termination (see [LPS] we can find a set W', a well-founded relation < on it, a ranking function ρ : States $\to$ W' and predicates Q_i, $i \in I$ satisfying the following (Q is defined to be $Q = \bigvee_{i \in I} Q_i$):

(M1) For every $s \in A$, $Q(s)$ holds

(M2) $Q(s) \wedge s' \in f_i(s) \supset Q(s') \wedge \rho(s) \geq \rho(s')$

(M3) $Q_i(s) \wedge s' \in f_j(s) \wedge \rho(s) = \rho(s') \supset Q_i(s')$

(M4) $Q_i(s) \wedge s' \in f_i(s) \supset \rho(s) > \rho(s')$

We may now define $W = W' \times (2^I - \{\emptyset\})$. If $v,v' \in W'$ and $K,K' \subseteq I$ we say that $(v,K) < (v',K')$ iff either $v < v'$ or $v=v'$ and $K' \subsetneq K$. This is a well-founded relation. We define $D_{(v,K)}$ as K and S_w as $I-D_w$, for $w \in W$. The predicate $p(s,(v,K))$ is defined as $a(s) \wedge \rho(s) = v \wedge K = \{i | i \in I, Q_i(s)\}$. Now we must check conditions (1)-(7).

(1) Obvious from the construction.

(2) Suppose w = v,K), s satisfies p(w) and B_j for $j \in K$, then s satisfies Q_j. By (M4) if state s' may result from the execution of C_j in state s, then $\rho(s') < \rho(s)$. By (b) s' satisfies a. By M2) the set $\{k | k \in I, Q_k(s')\} = L$ is not empty. Then s' satisfies p(u) for $u = (\rho(s'),L)$ and $u < w$. We have shown that $[p(w) \wedge B_j]\ C_j\ [\exists v < w\ p(w)]$ for $j \in D_w$.

We must now show that $p(w) \wedge B_j$ guarantees the termination of C_j. But every state satisfying p(w) satisfies a and is therefore reachable from some state satisfying r. Therefore < r > C <true> implies
$< p(w) \wedge B_j > C_j$ <true>.

(3) Suppose $w = (v,K)$, s satisfies $p(w)$ and B_k for $k \in I$. By the assumption concerning a, s may be reached from some state satisfying r (i.e. in A). By (M1) and (M2) then Q(s) holds. If state s' may result from the execution of C_k in state s, by (M2) we have Q(s') and $\rho(s) \geq \rho(s')$.
The set $L = \{i \in I | \ Q_i(s')\}$ is not empty (because Q(s') holds). By (b), we have a(s').
Therefore s' satisfies p(u) for $u = (\rho(s'),L)$, If $\rho(s) > \rho(s')$, $u < w$.
If $\rho(s) = \rho(s')$, by (M3) $L \supseteq K$ and $u \leq w$. We have shown

$$[p(w) \wedge B_k]\ C_k\ [\exists\, v \leq w, p(v)] \ .$$

But every state satisfying p(w) (and therefore a) is reachable from some state satisfying r and therefore <r> C <true> implies (3).

(4) If $|I| = 1$, $S_w = \emptyset$ and there is nothing to prove. Suppose $S_w \neq \emptyset$. Every state satisfying p(w) is reachable from some state satisfying r and therefore < r > C <true> implies (4), since every fair execution of the command in (4) is also a fair execution of C and since it has less guards than C.
(5) Let $w = (v,K)$ be a minimal element of W. It must be that v is a minimal element of W' and $K = I$. If s satisfies p(w), $Q_i(s)$ holds for every $i \in I$. Since the conclusion of (M4) cannot hold, we conclude that $f_i(s) = \emptyset$ for every $i \in I$. Suppose that s satisfies B_i, by definition of f_i this would imply that C_i has an infinite computation starting in s. But s is reachable from some state satisfying r and < r > C < q > . We conclude $\neg B_i(s)$ for every $i \in I$.

(6) Since $P(w) \supset a$ and $a \wedge \neg \bigvee_{i \in I} B_i \supset q$ (by (c)).
(7) If s satisfies r, it is in A. By (M1), Q(s) holds and the set $L = \{i \in I, \ \ Q_i(s)\}$ is not empty.

$w = (\rho(s),L)$ is then in W and s satisfies p(w) by (a). Q.E.D.

3. TOTAL CORRECTNESS UNDER THE ASSUMPTION OF JUSTICE

From now on, in place of the assumption of fairness as described in the introduction we shall make the weaker assumption of justice (weak fairness in [AO]). We assume that if, in the course of a non-terminating execution of the command C, from a certain time onwards, we find that every time we get at the beginning of the body of the loop the predicate B_i is true, then we will choose the command C_i for execution an infinite number of times.

We offer the following proof rule (another one may be found in [AO]). To prove $< r > \; C \; <q>$ (under the assumption of justice), find $W,<,p,F_w,S_w$ as before satisfying (1),(2),(3),(5),(6),(7) and

(4') For every $w \in W$, not a minimal element, and every $j \in D_w$,

$$p(w) \supset B_j \;\vee\; \neg \bigvee_{i\in I} B_i$$

We shall now show that our rule is sound and complete.

4. SOUNDNESS

Suppose there are $W, <, p, D_w$ satisfying (1)-(3),(4'),(5)-(7). Let $s_0,s_1,\ldots,s_n,\ldots$ be a sequence of states (finite or infinite) describing a computation of C , starting in a state satisfying r. By (7) $s_0 \models p(v_0)$ for some v_0. By (1),(2),(3) and (5) there is a non-increasing sequence: $v_0 \geq v_1 \geq \ldots \geq v_r \geq \ldots$ sucht that $s_r \models p(v_r)$, and $v_{i-1} > v_i$ if the i'th move was from $D_{v_{i-1}}$. If the sequence is finite, the last state s_n satisfies $\neg \bigvee_{i\in I} B_i$ and, by (6), satisfies q.

We must now show that no infinite execution of C may be just. If the sequence of v_i's is infinite then, from a certain point onwards, they must all be equal : $v_m = v_{m+1} = \ldots = v_n = \ldots$. Therefore no move from D_{v_m} was taken an infinite number of times. Since, by (1), D_{v_m} is not empty there is a $k \in D_{v_m}$ and C_k was taken only a finite number of times. By (4'), since $\forall n \geq, m$, $s_n \models p(v_m)$ and $s_n \models \bigvee_{i\in I} B_i$, we have $s_n \models B_k$ for every $n \geq m$. The computation is unjust.

5. COMPLETENESS

The proof proceeds along lines similar to that of Section 2. There is a one-to one correspondence between just computations of P and just executions of C. Therefore P justly terminates. By the completeness of method J we may find, W', <, ρ and Q_i's such that (M1)-(M4) and

$$\text{(J5)} \qquad Q_i(s) \supset f_i(s) \neq \emptyset \ \vee\ \forall i \in I \ \ f_i(s) = \emptyset \ .$$

Define $\quad W, <, p, D_w$ and S_w as in Section 2.

The proof of Section 2 shows that (1),(2),(3),(5),(6) and (7) hold (replace "fair" by "just" in the proofs). Let us show that (4') holds.

(4') Let $j \in D_w$, for $w = (u,K)$. If a state s satisfies p(w), then it satisfies Q_j. By (J5) then either $f_j(s) \neq \emptyset$ and therefore s satisfies B_j or $\forall i \in I$ $f_i(s) = \emptyset$. But for any $k \in I$, if s satisfies B_k then either $f_k(s) \neq \emptyset$ or there is a possible non-terminating computation of C_k starting in s, in contradiction with $< r > \ C < q >$. Q.E.D.

REFERENCES

[B] DE BAKKER, J.W., *Mathematical Theory of Program Correctness*, Prentice-Hall 1980.

[GFMR] GRUMBERG, O., N. FRANCEZ J. MAKOWSKY & W.P. DE ROEVER, *A proof rule for fair termination of guarded commands*, Proc. Int. Symp, on Algorithmic Languages (J.W. de Bakker & J.C. van Vliet, eds.), North-Holland, to appear.

[LPS] LEHMANN, D., A. PNUELI & J. STAVI, *Impartiality Justice and Fairness: the Ethics of Concurrent Termination*, Proc. ICALP 81 (S. Even & O. Kariv. eds), *Lecture Notes in Computer Science* 115, pp. 264-277, Springer, 1981.

[AO] APT, K.R. & E.R. OLDEROG, *Proof rules dealing with fairness*, Technical Report 8104, Institut fur Informatik und Praktische Mathematik, Christian-Albrechts Universität, Kiel, March 1981.