A First-Order Theory of Communication Multi-Agent Plans: Appendix B

Ernest Davis[*]
Courant Institute
New York University
davise@cs.nyu.edu

Leora Morgenstern
IBM Watson Labs
leora@us.ibm.com

March 6, 2005

Appendix B: Proof of correctness of plan

This document is appendix B to the paper, "A First-Order Theory of Communication and Multi-Agent Plans" by E. Davis and L. Morgenstern, to appear in *Journal of Logic and Computation.* In this section, we prove the correctness of plan el1. Not surprisingly, the proof, though long, is neither difficult nor deep; it consists mainly of forward projections with some case splitting, combined with a good deal of definition hunting. The value of the proof is that it gives some evidence by example that the axiomatic theory is sufficient to support the kinds of inference we want out of it. In practice, the exercise of constructing the proof led to substantial improvements of various kinds in the axiomatic theory.

One particular lemmas of general interest are encountered on the way; namely, lemma B.32 proves that an agent can always follow our protocol.

Note: Axioms T.4 – T.15 define durations and clock-times to be isomorphic to the integers. We will therefore use standard results of integer arithmetic without further justification.

Temporal lemmas

(Note: lemmas B.1 — B.7 are trivial and unoriginal. However, it is easier both for the authors and for the reader to re-prove them here than to hunt them down in the literature; and their triviality means that no substantive credit is being withheld from those who have proved them before.)

Definition BD.1: Situation $S1$ is a successor of $S0$, denoted "succ$(S1, S0)$" if $S1$ follows immediately after $S0$.

$$\text{succ}(S1, S0) \equiv S0 < S1 \wedge \neg\exists_S \; S0 < S < S1.$$

Lemma B.1: $\text{succ}(S1, S0) \Leftrightarrow \text{time}(S1)=\text{time}(S0)+1 \wedge S1 > S0.$

[*]The research reported in this paper was supported in part by NSF grant IIS-0097537.

Proof: Right to left: Suppose that time($S1$)=time($S0$)+1 and $S1 > S0$. By T.16, if $S0 < SM < S1$ then time($S0$) $<$ time(SM) $<$ time($S1$), but that is impossible. Since there can be no such SM it follows from BD.1 that succ($S1, S0$).

Left to right: Suppose that succ($S1, S0$). By T.16, time($S1$) $>$ time($S0$); since these are integers, time($S1$) $\geq$ time($S0$)+1. By T.18, there exists SM such that ordered($SM, S1$) and time(SM)=time($S0$)+1. By TD.2, T.2, T.3, T.16, $S0 < SM$. By T.16, $SM \leq S1$. By definition BD.1, it cannot be the case that $S0 < SM < S1$. Hence, $SM = S1$.

Lemma B.2: $\forall_{S0,SZ}\ S0 < SZ \Rightarrow \exists_S$ succ($S, S0$) $\wedge\ S \leq SZ$.

Proof: Using T.17 and T.18, let $S1$ be such that time($S1$) = time($S0$)+1 and ordered($S1, SZ$). By T.3, ordered($S1, S0$). By T.16, TD.2, $S0 < S1$. By B.1, succ($S1, S0$). By BD.1, $S1 \leq SZ$,

Lemma B.3: [ordered(SA, SB) $\wedge\ S0 < SB$] $\Rightarrow$ ordered($S0, SA$).

Proof: By TD.2, either $SA < SB$, $SA = SB$ or $SA > SB$. If $SA < SB$, the result follows from T.3; if $SA = SB$, the result is immediate; if $SA > SB$, the result follows from T.2.

Lemma B.4: [time($S0$) $<$ T $<$ time($S1$) $\wedge\ S0 < S1$] $\Rightarrow$
$\exists^1_{ST}$ time(ST)=T $\wedge\ S0 < ST < S1$.

Proof: By T.18, there exists ST such that ordered($ST, S1$) and time(ST)=T. By B.3 ordered($ST, S0$). By T.16, $S0 < ST < S1$. The uniqueness of ST follows from T.3, T.16.

Lemma B.5: (Induction from situations to intervals: Schema) Let $\phi(S)$ be a formula with an open situation variable S. Assume that the variable SF does not appear free in ϕ. Then the closure of the following formula holds:

$$[\phi(S0) \wedge \forall_S \phi(S) \Rightarrow \exists_{S1} \text{succ}(S1, S) \wedge \phi(S1)] \Rightarrow$$
$$\exists_I\ S0{=}\text{start}(I) \wedge \forall_S \text{elt}(S, I) \Rightarrow \phi(S).$$

Proof: Assume that the left hand of the implication holds for some s0. Let $\Gamma(S)$ be the formula, open in S, $\forall_{S1}$ s0 $\leq S1 \leq S \Rightarrow \phi(S)$. Then by assumption Γ(s0) and $\forall_S\, \Gamma(S) {\Rightarrow} \exists_{S1}\, S1 > S \wedge \Gamma(S1)$. From axiom I.5, it follows that there exists a u-interval i0 starting in s0 in which Γ holds infinitely often; i.e.

$$\text{s0}{=}\text{start(i0)} \wedge$$
$$\forall_S \text{ elt}(S,\text{i0}) \Rightarrow \exists_{S2}\ S < S2 \wedge \Gamma(S2) \wedge \text{elt}(S2,\text{i0}).$$

Now, lest sa be any situation in i0. We have shown that $\exists_{S2}$ sa $< S2 \wedge \Gamma(S2)$; but, by definition of Γ, that means that ϕ(sa).

Lemma B.6: (Existence of a "first" situation after $S0$ satisfying ϕ.) (Schema) Let $\phi(S)$ be a formula with an open situation variable S. Assume that the variable SF does not appear free in ϕ. Then the closure of the following formula holds:

$$\phi(S1) \wedge S0 < S1 \Rightarrow$$
$$\exists_{SF}\ \phi(SF) \wedge S0 \leq SF \wedge \forall_S\ S0 \leq S < SF {\Rightarrow} \neg\phi(S).$$

Proof: Assume that $S0 < S1$ and $\phi(S1)$. For any duration D, let $\Gamma(D)$ be the formula,

$$\exists_{SD} \text{ time}(SD) = \text{time}(S0) + D \wedge S0 \leq SD \leq S1 \wedge \phi(SD)$$

By assumption $\Gamma(D1)$ holds for $D1$=time($S1$)$-$time(S). Hence there is some smallest positive value DF such that $\Gamma(DF)$. By construction of Γ, there exists an SF such that time(SF)=DF, $S0 \leq SF$

and $\phi(SF)$. Let S be any situation such that $S0 \leq S < SF$, and let D=time(S)−time($S0$). Since $D < DF$, we must have $\neg\Gamma(D)$. Since $S0 \leq S < S1$, we must have $\neg\phi(SD)$.

Lemma B.7: $T1 \geq$time(start(I)) $\Rightarrow \exists_{S1}$ elt($S1, I$) $\wedge$ $T1$=time($S1$).

Proof: Let i0 be an interval, let s0=start(i0), and let t0=time(s0). Let $\Phi(D)$ be the formula "$\exists_S$ time(S)=t0+D $\wedge$ elt(S,i0)". Clearly, since elt(s0,i0), it follows that $\Phi(0)$. Suppose, inductively, that $D1 \geq 0$ and $\Phi(D1)$. Then there exists a situation SX such that time(SX)=t0+$D1$ and elt(SX,i0). Let $S1$ be any successor to SX. By I.4, there exists a situation $S2$ such that $\neg(S2 < S1)$ and elt($S2$,i0). By T.18, there exists a situation SM such that time(SM)=t0+D+1 and ordered($SM, S2$). Using T.16, it follows that in fact $SX < SM \leq S2$, so by I.2, elt(SM,i0). Thus $\Phi(D1 + 1)$. Using induction on durations (T.15), it follows that $\Phi(D)$ for all $D \geq 0$, which gives the desired result. Uniqueness follows from I.1 and T.16.

Lemmas on actions and knowledge

Lemma B.8:
[action($E1, A$) $\wedge$ action($E2, A$) $\wedge$ leads_toward($E1, S0, S1$) $\wedge$ leads_toward($E2, S0, S2$) $\wedge$
ordered($S1, S2$)] $\Rightarrow$
$E1 = E2$.

Proof: Immediate from A.1, EVD.1, AD.2, when time($S0$) > 0t; from A.6, AD.3 when time($S0$)=0t.

Lemma B.9: action(E, A) $\wedge$ occurs($E, S1, S2$) $\Rightarrow$ choice($A, S2$).

Proof: From A.2, AD.3.

Lemma B.10: $S0 < S1 < S2 \wedge S1 < SX$ $\wedge$ occurs($E, S0, S2$) $\wedge$ action(E, A) $\Rightarrow$
$\exists_{SY}$ ordered(SX, SY) $\wedge$ occurs($E, S0, SY$).
(If $S1$ is in the middle of the execution of E (between $S0$ and $S2$) then this execution is completed along every time line that contains $S1$.)

Proof: By EVD.1 leads_towards($E, S0, S1$). By axiom A.1, $\exists^1_{E1}$ action($E1, A$) $\wedge$ leads_toward($E1, S0, SX$). By EVD.1, there exists SY such that occurs($E1, S0, SY$) and ordered(SY, SX). By lemma B.3, ordered($SY, S1$). By EVD.1, leads_towards($E1, S0, S1$). But by A.1, the action of A that leads from $S0$ toward $S1$ is unique; hence $E1 = E$.

Lemma B.11:
$\forall_{A,S0,S2}$ $S0 < S2 \Rightarrow$
$\exists_{SX,E,SY}$ $SX \leq S0 < SY$ $\wedge$ action(E, A) $\wedge$ occurs(E, SX, SY) $\wedge$ ordered($SY, S2$).
(Any situation $S0$ occurs either at the beginning or in the middle of an action E that starts in SX before or at $S0$, and that continues along every time line (toward $S2$) containing $S0$.)

Proof: If choice($A, S0$) then choose $SX = S0$. By axiom A.1 there exists an action E of A such that leads_toward($E, S0, S2$); that is, by EVD.1, there exists SY such that ordered($SY, S2$) and occurs($E1, S0, SY$).

Otherwise, if not choice($A, S0$), then by AD.3 and AD.1 there exists SX, SZ, E such that action(E, A), $SX < S0 < SZ$ and occurs(E, SX, SZ). The result then follows from lemma B.10.

Lemma B.12:
$\forall_{A,S0,S2}$ $S0 < S2 \Rightarrow$
$\exists_{SY}$ choice(A, SY) $\wedge$ $S0 < SY$ $\wedge$ ordered($SY, S2$) $\wedge$ time(SY) $\leq$ time($S0$) + max_action_time.
(On any time line, choice points for A occurs with a maximum gap of max_action_time.)

Proof: By lemma B.11, there exist E, SX, SY such that action(E, A), occurs(E, SX, SY), $SX \leq S0 < SY$ and ordered($SY, S2$). By M.1, time(SY) $\leq$ time(SX)+max_action_time $\leq$ time($S0$) +

max_action_time.

Lemma B.13:
$\text{elt}(S, I) \Rightarrow$
$\exists_{S1}\ S < S1 \wedge \text{elt}(S1, I) \wedge \text{choice}(A, S1) \wedge \text{time}(S1) \leq \text{time}(S) + \text{max\_action\_time}$.

Proof: By lemma B.7, there exists $S2$ in I such that $\text{time}(S2) = \text{time}(S) + \text{max\_action\_time}$. The result then follows from B.12.

Lemma B.14: $\text{k\_acc}(A, S0, S0A) \Rightarrow \text{time}(S0) = \text{time}(S0A)$.

Proof by contradiction. Suppose this is false. Since k_acc is symmetric by axiom K.3, there exists $A, S0, S0A$ for which $\text{k\_acc}(A, S0, S0A)$ and $\text{time}(S0) < \text{time}(S0A)$. Let t1 be the earliest time for which there exists a, s1, s1a such that k_acc(a,s1,s1a) and t1=time(s1) < time(s1a). Using T.18, choose an sa such that time(sa)=t1, sa < s1a. Using K.3, K.4 there exists a situation s such that k_acc(a,sa,s), s < s1. By T.16, time(s) < time(s1). But then, by K.3, we have k_acc(a,s,sa) and time(s) < time(sa) = t1, contradicting the assumption that t0 was the earliest time when this could happen.

Lemma B.15: $[\text{k\_acc}(A, SXA, SXB) \wedge \text{occurs}(E, SXA, SYA) \wedge \text{action}(E, A)] \Rightarrow$
$\exists_{SYB}\ \text{occurs}(E, SXB, SYB)$.

Proof: By K.5, there exists $S1B, S2B$ such that $\text{k\_acc}(A, SXA, S1B)$, $S1B \leq SXB$, and $\text{occurs}(E, S1B, S2B)$. (Bind $S1A$ in K.5 to SXA here; $S2A$ to SYA; SA to SXA and $S2B$ to SXB.) By lemma B.14, $\text{time}(SXA) = \text{time}(SXB) = \text{time}(S1B)$. By TD.3, T.10, T.16, $SXB = S1B$.

Lemma B.16: $\text{choice}(A, S1) \wedge \text{k\_acc}(A, S1, S1A) \Rightarrow \text{choice}(A, S1A)$.
(You know when you're at a choice point.)

Proof: By AD.1 and AD.2, there exist $E, S2$ such that $\text{action}(E, A)$ and $\text{occurs}(E, S1, S2)$. By lemma B.15 there exists $S2A$ such that $\text{occurs}(E, S1A, S2A)$. By AD.1, AD.2 $\text{choice}(A, S1A)$.

Lemma B.17: $[\forall_{SA}\ \text{k\_acc}(A, S, SA) \Rightarrow \text{choice}(A, SA)] \vee [\forall_{SA}\ \text{k\_acc}(A, S, SA) \Rightarrow \neg\text{choice}(A, SA)]$.
(You know whether you're at a choice point.)

Proof: Immediate from K.2 and lemma B.16.

Lemma B.18:
$[\text{action}(E, A) \wedge \text{k\_acc}(A, S0, S0A) \wedge \text{feasible}(E, S0)] \Rightarrow$
$\text{feasible}(E, S0A)$.

Proof: By EVD.2 there exists $S1$ such that $\text{occurs}(E, S0, S1)$. By lemma B.15, there exists $S1A$ such that $\text{occurs}(E, S0A, S1A)$. By EVD.2, $\text{feasible}(E, S0A)$.

Lemma B.19:
$[\text{k\_acc}(A, S, SA) \wedge \text{action}(E, A)] \Rightarrow [\text{engaged}(E, A, S) \Leftrightarrow \text{engaged}(E, A, SA)]$.
(You know whether you're engaged in action E.)

Proof: From axioms AD.1 and K.5.

Definition BD.2: $\text{know\_whether}(A, Q, S) \equiv$
$[\forall_{SA}\ \text{k\_acc}(A, S, SA) \Rightarrow \text{holds}(SA, Q)] \vee [\forall_{SA}\ \text{k\_acc}(A, S, SA) \Rightarrow \neg\text{holds}(SA, Q)]$

(A knows whether Q holds in S means that either A knows in S that Q holds in S or A knows in S that Q does not hold in S.)

Definition BD.3:
$\text{k\_acc\_int}(A, S1, S2, S1A, S2A) \equiv$
$\text{k\_acc}(A, S1, S1A) \wedge \text{k\_acc}(A, S2, S2A) \wedge S1 < S2 \wedge S1A < S2A$.
(Interval $[S1A, S2A]$ is knowledge accessible from $[S1, S2]$.)

Lemma B.20:
$[\forall_S \text{ know\_whether}(AC, Q, S)] \Rightarrow$
$[\forall_{S0A,S1A} \text{ [k\_acc\_int}(AC, S0, S1, S0A, S1A) \Rightarrow \text{opportunity}(S1A, AC, AR, Q)]] \vee$
$[\forall_{S0A,S1A} \text{ [k\_acc\_int}(AC, S0, S1, S0A, S1A) \Rightarrow \neg\text{opportunity}(S1A, AC, AR, Q)]]$
(If AC always knows whether Q is true, then he always know whether $S1$ is an opportunity to act on Q.)

Proof: From MD.2, lemma B.17, and lemma B.14.

Lemma B.21:
$[\forall_S \text{ know\_whether}(AC, Q, S)] \Rightarrow$
$[\forall_{S0A,S1A} \text{ [k\_acc\_int}(AC, S0, S1, S0A, S1A) \Rightarrow \text{first\_opportunity}(S1A, AC, AR, S0A, Q)]] \vee$
$[\forall_{S0A,S1A} \text{ [k\_acc\_int}(AC, S0, S1, S0A, S1A) \Rightarrow \neg\text{first\_opportunity}(S1A, AC, AR, S0A, Q)]]$
(If AC always knows whether Q is true, then he always know whether $S1$ is the first opportunity to act on Q.)

Proof: From MD.3, lemma B.20, and K.4.

Lemmas about plans

Lemma B.22: $\text{begin\_plan}(P, AC, AR, S0, S1) \wedge S0 \leq SM < S1 \Rightarrow \text{begin\_plan}(P, AC, AR, S0, SM)$.

Proof: From QD.6

Lemma B.23:
$\text{attempt\_toward}(P, AC, AR, S0, S1) \wedge S0 \leq SM < S1 \Rightarrow \text{attempt\_toward}(P, AC, AR, S0, SM)$.

Proof: Assume that attempt_toward(p,ac,ar,s0,s1) and that s0≤sm<s1. By QD.8, either begin_plan(p,ac,ar,s0,s1) or for some s2 between s0 and s1, begin_plan(p,ac,ar,s0,s2) and terminates_plan(p,ac,ar,s0,s2). There are three cases to consider:

Case 1: begin_plan(p,ac,ar,s0,s1). By lemma B.22, begin_plan(p,ac,ar,s0,sm). By QD.8, attempt_toward(p,ac,ar,s0,sm).

Case 2: begin_plan(p,ac,ar,s0,s2), terminates_plan(p,ac,ar,s0,s2), and sm≥s2. Then, by QD.8, attempt_toward(p,ac,ar,s0,sm).

Case 3: begin_plan(p,ac,ar,s0,s2), terminates_plan(p,ac,ar,s0,s2), and sm<s2. Then, by lemma B.22, begin_plan(p,ac,ar,s0,sm), so by QD.8, attempt_toward(p,ac,ar,s0,sm).

Lemma B.24:
$[\text{begin\_plan}(P, AC, AR, S0, S1) \wedge \text{choice}(AC, S1) \wedge \neg\text{terminates}(P, AC, AR, S0, S1) \wedge$
$\text{know\_next\_step}(E, P, AC, S0, S1) \wedge \text{leads\_towards}(E, S1, S2) \wedge \text{succ}(S2, S1)] \Rightarrow$
$\text{begin\_plan}(P, AC, AR, S0, S2)$

Proof: This together with lemma B.25 are, so to speak, the recursive restatement of definition QD.6. That is, these two lemmas define $\text{begin\_plan}(P \ldots S2)$ recursively in terms of $\text{begin\_plan}(P \ldots S1)$ where $S1$ is the predecessor of $S2$.

Assume that the left-hand side of the above implication holds. By QD.6, since $\text{begin\_plan}(P, AC, AR, S0, S1)$ we have $S0 \leq S1$. Since $\text{succ}(S2, S1)$ it follows that $S0 < S2$.

For any intermediate situation SM and for a final situation SZ either equal to $S1$ or $S2$, let us abbreviate the condition

$\neg\text{terminates}(P, AC, AR, S0, SM) \wedge$

[choice$(AC, SM) \Rightarrow$
$\exists_E$ know_next_step$(E, P, AC, S0, SM) \wedge$ leads_towards(E, SM, SZ)]

on the right-hand side of QD.6 as $\Phi_{P,AC,AR,S0}(SM, SZ)$. By QD.6, we know that $\Phi(SM, S1)$ holds for all SM such that $S0 \leq SM < S1$. Also by QD.6, if we can establish that $\Phi(SM, S2)$ holds for all SM such that $S0 \leq SM < S2$, then we have established the desired result begin_plan$(P, AC, AR, S0, S2)$. There are three cases:

Case 1: $S0 \leq SM < S1$ and choice(AC, SM). Since $\Phi(SM, S1)$, there exists E such that know_next_step$(E, P, AC, S1, SM)$ and leads_toward$(E, SM, S1)$. By assumption, we have choice$(AC, S1)$. Therefore the condition leads_toward$(E, SM, S1)$ implies that occurs(E, SM, SN) for some $SN \leq S1 < S2$, so we have leads_toward$(E, SM, S2)$. Thus we have established all parts of $\Phi(SM, S2)$.

Case 2: $S0 \leq SM < S1$ and $\neg$choice(AC, SM). Thus, in this case $\Phi(SM, S2)$ requires only that $\neg$terminates$(P, AC, AR, S0, SM)$, which we know from $\Phi(SM, S1)$.

Case 3: $SM = S1$. $\Phi(S1, S2)$ is explicitly stated on the left side of the implication in the statement of our lemma.

Lemma B.25:
[begin_plan$(P, AC, AR, S0, S1) \wedge \neg$choice$(AC, S1) \wedge$
$\neg$know_succeeds$(P, AC, S0, S1) \wedge$ succ$(S2, S1)] \Rightarrow$
begin_plan$(P, AC, AR, S0, S2)$.

Proof: By QD.3, QD.4, QD.5, P can only terminate in $S1$ if either choice$(AC, S1)$ or know_succeeds$(P, AC, S0, S1)$. The result then follows from QD.6.

Lemma B.26:
[begin_plan$(P, AC, AR, S0, S1) \wedge S0 \leq SM < S1 \wedge$ leads_towards$(E, SM, S1) \wedge$ action$(E, AC)] \Rightarrow$
know_next_step$(E, P, AC, S0, SM)$.

Proof: By EVD.1, AD.2, and AD.3, choice(AC, SM). By QD.6, there is an action $E1$ in SM which A knows to be a next step of P and which leads toward $S1$. By P.1, $E1$ is an action of AC. By A.1, $E1 = E$. Hence, AC knows in SM that E is a next step of P.

Lemma B.26.A: $\forall_{S1,S2}\ S1 < S2 \wedge$ soc_poss$(S2) \Rightarrow$ soc_poss$(S1)$.

Proof: From QD.9 and lemma B.23.

Lemma B.27:
$[D1 \geq 0 \wedge D2 \geq 0 \wedge T \leq T2 \leq T + D1 \wedge$ reserved_block$(T, AC, AR, D1 + D2)] \Rightarrow$
reserved_block$(T2, AC, AR, D2)$

Proof: From QD.1 with arithmetic.

Lemma B.28: [working_on$(P, AC, AR, S0, S1) \wedge S0 \leq SB \leq S1] \Rightarrow$ working_on$(P, AC, AR, S0, SB)$.

Proof: From Q.5, QD.6, and lemma B.22.

Lemma B.29:
[working_on$(PX, AC, AR, SX, S) \wedge$ working_on$(PY, AC, AR, SY, S)] \Rightarrow$
$PY = PX \wedge SY = SX$.
Agent AC works on at most one plan of agent AR's at a time.

Proof: From Q.5, we have $SX \leq S$, accepts_req(PX, AC, AR, SX), $SY \leq S$, accepts_req(PY, AC, AR, SY). By T.3, either $SX \leq SY$ or $SY \leq SX$. Assume without loss of generality that $SX \leq SY$. By lemma B.28, working_on(PX, AC, AR, SX, SY). By Q.6 since accepts_req(PY, AC, AR, SY), it follows that $\forall_{PQ,SQ}$ working_on(PQ, AC, AR, SQ, SY) $\Rightarrow PQ = PY$, $SQ = SX$. Hence $PX = PY$, $SX = SY$.

Lemma B.30
[working_on($P, AC, AR, S0, S1$) $\wedge$ action(E, AC) $\wedge$ $S0 \leq SM$ $\wedge$ leads_toward($E, SM, S1$)] $\Rightarrow$ know_next_step($E, P, AC, S0, SM$).

Proof: Immediate from Q.5 and lemma B.26.

Lemma B.31
[$\neg\exists_{S0}$working_on($P, AC, AR, S0, S1$)] $\wedge$ working_on($P, AC, AR, S2, S3$) $\wedge$ $S1 < S3 \Rightarrow$
$S1 < S2 \wedge \exists_{SX}$ occurs(request(AC, AR, P),$SX, S2$).
(If AC goes from not working on P in $S1$ to working on P from $S2$ to $S3$, then a request to do P must have completed at $S2$.)

Proof: Since working_on($P, AC, AR, S2, S3$), by Q.5 accepts_req($P, AC, AR, S2$). By lemma B.28, for all SB between $S2$ and $S3$, working_on($P, AC, AR, S2, SB$). Hence $S1$ is not between $S2$ and $S3$, so $S1 < S2$. By Q.6 there exists an SX such that occurs(request(P, AC, AR),$SX, S2$).

Definition BD.4.:
good_action($E, AC, S1$) $\equiv$
choice($AC, S1$) $\wedge$ $\forall_{P,AR,S0}$ [working_on($P, AC, AR, S0, S1$) $\Rightarrow$ know_next_step($E, P, AC, AR, S0, S1$)].
Action E is a good action for AC in $S1$ if it is a continuation of every plan P that AC is currently working on.

Lemma B.32: $\forall_{AC,S}$ choice(AC, S) $\Rightarrow$ $\exists_E$ good_action(E, AC, S).

"There is one thing, Emma, that a man can always do if he chooses, and that is, his duty." (Jane Austen)

Proof: A hierarchical case analysis

Case 1. Suppose there exist $AR, P, S0$ such that AC reserves time(S) for AR and working_on($P, AC, AR, S0, S$).

By axiom Q.1 and lemma B.29 there is at most one such AR, P, and $S0$.

Case 1.1 : Suppose there is an action E such that exec_cont($E, P, AC, AR, S0, S$).
By QD.2, know_next_step($E, P, AC, AR, S0, S$). Let $PX \neq P, ARX, S0X$ be any values such that working_on($PX, AC, ARX, S0X, S$). By lemma B.29, $ARX \neq AR$, so by Q.1, $\neg$reserved(time(S), AC, ARX). By QD.2 $\neg$governs(ARX, E) and by PD.1 feasible(E, S).
Since working_on($PX, AC, ARX, S0X, S$), by Q.5 $\neg$terminates($PX, AC, ARX, S0X, S$). By QD.5 $\neg$abandon2($P, AC, ARX, S0X, S$). By QD.4, for any action $E1$, if action($E1, AC$) and $\neg$governs($ARX, E1$) then know_next_step($E1, P, AC, S0X, S$). In particular know_next_step($E, P, AC, S0X, S$).
Since the implication "working_on($PX, AC, ARX, S0X, S$) $\Rightarrow$ know_next_step($E, PX, AC, S0X, S$)" holds for all $PX, ARX, S0X$, we have good_action(E, AC, S) (definition BD.4).

Case 1.2 Suppose that there is no action E such that exec_cont($E, P, AC, AR, S0, S$). By QD.3, abandon1($P, AC, AR, S0, S$). By QD.5, terminates($P, AC, AR, S0, S$). But by Q.5 this contradicts the assumption that working_on($P, AC, AR, S0, S$).

Case 2. Suppose that reserved(time(S),AC, AR) and choice(AC, S), but there is no plan P and situation $S0$ such that working_on($P, AC, AR, S0, S$). Let E=do(AC,wait), so E is not governed by any agent (Q.4). Let $PX, ARX, S0X$ be any values such that working_on($PX, AC, ARX, S0X, S$). Then we can prove that know_next_step($E, PX, AC, S0X, S$) using exactly the same argument as in case 1.1.

Case 3. Suppose that time(S) is not reserved for any agent AR. Let E=do(AC,wait), so E is not governed by any agent (Q.4). Let $PX, ARX, S0X$ be any values such that working_on($PX, AC, ARX, S0X, S$). Then, again, we can prove that know_next_step($E, PX, AC, ARX, S0X, S$) using exactly the same argument as in the second part of case 1.1. ∎

Lemma B.33: soc_poss($S1$) $\wedge$ $S < S1$ $\wedge$ leads_towards($E, S, S1$) $\wedge$ action(E, AC) $\Rightarrow$ good_action(E, AC, S).
(In a "socially possible" history, all actions are good.)

Proof: Assume that the left-hand side of the implication is satisfied, We need to prove that good_action(E, AC, S); that is, by definition BD.4,

choice(AC, S) $\wedge$ $\forall_{P,AR,S0}$ working_on($P, AC, AR, S0, S$) $\Rightarrow$
know_next_step($E, P, AC, S0, S$)

It is immediate from AD.2, EVD.2 that choice(AC, S) Assume that working_on($P, AC, AR, S0, S$) Clearly $S0 \leq S < S1$. By Q.5 we have accepts_req($P, AC, AR, S0$), begin_plan($P, AC, AR, S0, S$) and $\neg$terminates($P, AC, AR, S0, S$). By QD.8, attempt_toward($P, AC, AR, S0, S$). Since begin_plan($P, AC, AR, S0, S$), by QD.6 $\forall_{SM}$ $S0 \leq SM < S \Rightarrow \neg$terminates($P, AC, AR, S0, SM$). Since leads_towards($E, S, S1$) there exists $S2$ such that occurs($E, S, S2$) and ordered($S2, S1$). Let $S4$ be such that succ($S4, S$) and $S4 \leq S2$. Clearly $S4 \leq S1$. By lemma B.26.A, soc_poss($S4$). By QD.9 attempt_toward($P, AR, AC, S0, S4$). But we have, for all SM such that $S0 \leq SM \leq S$, $\neg$terminates($P, AC, AR, S0, SM$). Hence by QD.8, begin_plan($P, AC, AR, S0, S4$). Since E is the unique action such that leads_toward($E, S0, S4$), it follows from QD.6 that know_next_step($E, P, AC, S0, S$).

Lemma B.34:
$[\forall_{S,AC,E}$ $[S < S1 \wedge$ action(E, AC) $\wedge$ leads_towards($E, S, S1$)$]$ $\Rightarrow$ good_action(E, AC, S)$]]$ $\Rightarrow$ soc_poss($S1$).
(If all actions before $S1$ are good, then $S1$ is socially possible.)

Proof of the contrapositive: Suppose that $\neg$soc_poss($S1$). By QD.9, there exist $S0, P, AC, AR$ such that $S0 < S1$, accepts_req($P, AC, AR, S0$) and $\neg$attempt_toward($P, AC, AR, S0, S1$). By QD.8 $\neg$begin_plan($P, AC, AR, S0, S1$). By QD.6 begin_plan($P, AC, AR, S0, S0$). Let $S3$ be the last situation such that $S0 \leq S3 < S1$ and begin_plan($P, AC, AR, S0, S3$). Since $\neg$attempt_toward($P, AC, AR, S0, S1$), it follows from QD.8 that $\neg$terminates($P, AC, AR, S0, S3$); and from QD.5 that $\neg$know_succeeds($P, AC, S0, S3$). From lemma B.25 it follows that choice($AC, S3$). From Q.5 we have working_on($P, AC, AR, S0, S3$). Let event E be such that leads_toward($E, S3, S1$), and suppose that occurs($E, S3, S4$), where ordered($S4, S1$). Let $S5$ be the earlier of $S1$ and $S4$; then $S3 < S5 \leq S1$.

Since we defined $S3$ to be the last situation such that $S0 \leq S3 < S1$ and begin_plan($P, AC, AR, S0, S3$), it follows that $\neg$begin_plan($P, AC, AR, S0, S5$). By the contrapositive to lemma B.24, E must not be a continuation of P in $S3$; hence, by definition BD.4, E is not a good action in $S3$. Thus, we have established that if $\neg$soc_poss($S1$) then there exist $E, S3, P, AC$, such that $S3 < S1$, action(E, AC), leads_towards($E, S3, S1$), and $\neg$good_action($E, AC, S3$), which is just the contrapositive of the statement of the lemma.

Lemma B.35: soc_poss($S1$) $\Leftrightarrow$
$\forall_{S,AC,E}$ $[S < S1 \wedge$ action(E, AC) $\wedge$ leads_towards($E, S, S1$)$]$ $\Rightarrow$ good_action(E, AC, S).
($S1$ is socially possible if and only if all actions before $S1$ are good.)

Proof: From B.33 and B.34.

Lemma B.36:
[accepts_req($P, AC, AR, S0$) $\wedge$ $S1 > S0$ $\wedge$ soc_poss($S1$)] $\Rightarrow$
[working_on($P, AC, AR, S0, S1$) $\vee$

$[\exists_{SM}\ S0 \leq SM \leq S1 \wedge \text{begin\_plan}(P, AC, AR, S0, SM) \wedge \text{terminates}(P, AC, AR, S0, SM)]]$.

Proof: Assume that the left-hand side of the implication holds. By QD.9, attempt_toward($P, AC, AR, S0, S1$). By QD.8, either P begins over the interval $[S0, S1]$ or it finishes over some initial segment $[S0, SM]$. The second possibility is the second disjunct of the right-hand side of our lemma. If P does not finish over $[S0, S1]$ initial segment and P begins over $[S0, S1]$ then by Q.5 AC is working on P in $S1$.

Lemma B.37: soc_poss($S0$) $\Rightarrow \exists_{S1}$ succ($S1, S0$) $\wedge$ soc_poss($S1$).

Proof: Assume that soc_poss($S0$). If $S0$ is a choice point for agent A, then using lemma B.32, let E be an action such that good_action(E, A, S) and let $S1$ be a situation such that leads_towards($E, S, S1$) and succ($S1, S$). If S is not a choice point for any agent A, let $S1$ be any situation such that succ($S1, S$). By B.35, since soc_poss($S0$), all actions before $S0$ are good actions; by the above constructions, the action, if any, at $S0$ is a good action. Thus, all actions before $S1$ are good actions, so by lemma B.35, soc_poss($S1$).

Lemma B.38 soc_poss(S) $\Rightarrow \exists_I$ S=start(I) $\wedge$ soc_poss_int(I).
(Any soc_poss situation S can be extended to an unbounded soc_poss interval I.)

Proof: From lemmas B.37 and B.5.

Validation of plan el2

Lemma B.39:
k_acc($A, S1, S1A$) $\wedge T0 <$ time($S1$) $\Rightarrow$ holds($S1$,loaded_since($B, A, T0$)) $\Leftrightarrow$ holds($S1A$,loaded_since($B, A, T0$)).

Proof: From XD.10, E.19, E.21, K.4, and lemma B.19.

Lemma B.40:
$[\forall_{S0A,SA}$ k_acc_int($A, S0, S, S0A, SA$) $\Rightarrow \Phi(A, SA, S0A)] \vee$
$[\forall_{S0A.SA}$ k_acc_int($A, S0, S, S0A, SA$) $\Rightarrow \neg\Phi(A, SA, S0A)]$
where Φ is any of "el2_q1f", "el2_q1", "el2_q2f", "el2_q2", and "el2_q3".
(Agent A always knows whether any of the above conditions hold.)

Proof: From lemma B.21, B.14 together with E.20, E.21, and XD.6 through XD.11.

Lemma B.41:
[$AZ \neq$ hero $\wedge$ el2_q1($AZ, S2, S1$)] $\Rightarrow$
[know_next_step(E,el2(AZ),AZ,$S2, S1$) $\Leftrightarrow$ E=do(AZ,call)].

Proof: By X.6, the only next step of el2(AZ) in $S2$ is do(AZ,call). By E.15, this action is possible. By lemmas B.40 and B.18 and axiom E.19, AZ knows that this is the only next step and knows that it is possible.

Lemma B.42:
[$AZ \neq$ hero $\wedge$ el2_q2($AZ, S2, S1$)] $\Rightarrow$
[know_next_step(E,el2(AZ),AZ,$S2, S1$) $\Leftrightarrow$ E=do(AZ,load(b1))].

Proof: Analogous to lemma B.41.

Lemma B.43:
[holds($S1$,has(AZ, B)) $\wedge$ $\neg$holds($S2$,has(AZ, B)) $\wedge$ $S1 < S2$] $\Rightarrow$
holds($S2$, loaded_since(B, AZ,time($S1$)))

Proof: By E.17 there exist $S3, S4$ such that $S3 < S2$, $S1 < S4$, ordered($S2, S4$) and occurs(do(AZ,load(B)),$S3, S4$). By E.5 there exists $SM < S4$ such that throughout($SM, S4$,on_elevator(B)). Let SA be the earlier of $SM, S2$; thus $SA < S4$ and $SA \leq S2$. By E.9, holds(SA,elevator_at(AZ)). Hence, by XD.10, holds($S2$, loaded_since(B, AZ,time($S1$))

Lemma B.44:
[$AZ \neq$ hero $\wedge$ el2_q3($AZ, S2, S1$)] $\Rightarrow$
[know_next_step(E,el2(AZ),AZ,$S2, S1$) $\Leftrightarrow$
instance(E,inform(AZ, robots, loaded_since(b1,AZ,time($S1$))),$S2$)]

Proof: Analogous to lemma B.41.

Lemma B.44.A:
el2_q3($AZ, S2, S1$) $\Rightarrow$
$\exists_E$ instance(E,inform(AZ, robots, loaded_since(b1,AZ,time($S1$))),$S2$) $\wedge$ feasible($E, S2$).

Proof: Let QL be the fluent loaded_since(b1,AZ,time($S1$)). By axiom E.16, it is feasible for AZ to communicate to robots. By lemma B.39, AZ knows in $S2$ that QL. By C.1, inform(AZ,robots,QL) is feasible in $S2$. By C.4, know_how(AZ,inform(AZ,robots,QL),$S2$). The result follows from MD.1 and KHD.1.

Lemma B.45:
[$AZ \neq$ hero $\wedge$ choice($AZ, S1$) $\wedge$
$\neg$el2_q1($AZ, S2, S1$) $\wedge$ $\neg$el2_q2($AZ, S2, S1$) $\wedge$ $\neg$el2_q3($AZ, S2, S1$)] $\Rightarrow$
[next_step(E,el2(AZ),$S1, S2$) $\Leftrightarrow$ [action(E, AZ) $\wedge$ $E \neq$do(AZ,unload(b1))]].

Proof: From X.6.

Lemma B.46:
[$AZ \neq$ hero $\wedge$ choice($AZ, S1$) $\wedge$
$\neg$el2_q1($AZ, S2, S1$) $\wedge$ $\neg$el2_q2($AZ, S2, S1$) $\wedge$ $\neg$el2_q3($AZ, S2, S1$)] $\Rightarrow$
[know_next_step(E,el2(AZ),AZ,$S1, S2$) $\Leftrightarrow$
[action(E, AZ) $\wedge$ $E \neq$do(AZ,unload(b1)) $\wedge$ feasible($E, S2$)]

Proof: By lemma B.45, any action of AZ other than unload(b1) is a next step of el2(AZ). By lemmas B.17 and B.40, AZ knows that the conditions on the left-hand side of the implication hold, and (using lemma B.45) therefore knows that any action other than unload(b1) is next step of el2(AZ).

Lemma B.47: $\neg$abandon2(el2(AZ),AZ,hero,$S1, S2$)

Proof: By QD.4, if reserved(time($S2$),AZ,hero), then $\neg$abandon2(el2(AZ),AZ,hero,$S1, S2$). Suppose that $\neg$reserved(time($S2$),AZ,hero). By MD.2, MD.3, XD.7, XD.9, XD.11, none of the conditions el2_q1($AZ, S1, S2$), el2_q2($AZ, S1, S2$), el2_q3($AZ, S1, S2$) hold. Let $S1A$ and $S2A$ be knowledge accessible from $S1$ and $S2$ respectively. By lemma B.40, none of the conditions el2_q1($AZ, S1A, S2A$), el2_q2($AZ, S1A, S2A$), el2_q3($AZ, S1A, S2A$) hold. By X.6, any action other than "unload(b1)" is a next step of el2(AZ) in $S2A$. By E.22, X.9, this includes every action not governed by hero. The result follows from QD.4, PD.1.

Lemma B.48:
terminates(el2(AZ),AZ,hero,$S1, S2$) $\Leftrightarrow$ $S2 > S1$ $\wedge$ time($S2$) $\geq$ time($S1$) + max_el2b_time.

Proof: By QD.5, el2(AZ) terminates in $S2$ iff it is known to succeed or it is abandoned. From lemmas B.41, B.42, B.44, B.45, B.46, with definition QD.3, it follows that el2(AZ) is not abandoned type 1 in $S2$. Lemma B.47 states that el2(AZ) is not abandoned type 2 in $S2$. From X.5 and lemma B.14, el2(AZ) is known to succeed if time($S2$) $\geq$ time($S1$) + max_el2b_time.

Lemma B.49:
[$AZ \neq$hero $\wedge$ working_on(el2(AZ),AZ,hero,$S0, S1$)] $\Rightarrow$
$\neg\exists_{S2}$ $S0 \leq S2 < S1$ $\wedge$ leads_toward(do(AZ,unload(b1)), $S2, S1$).

Proof: By X.6 do(AZ,unload(b1)) is never a next step of el2(AZ). The result follows from lemma B.30, PD.1, and K.1.

Lemma B.50:
[holds($S1$, loaded_since(b1,$A2$,time($S0$))) $\wedge$
 [$\forall_{AZ}$ AZ $\neq$hero $\Rightarrow$ working_on(el2(AZ),AZ,hero,$S0, S1$)]] $\Rightarrow$
holds($S1$,on_elevator(b1)) $\vee$ holds($S1$,has(hero,b1)).

Proof: By E.12, in $S1$, either b1 is on the elevator or some agent has b1. By XD.10 there exists a situation SA between $S0$ and $S1$ such that in SA, b1 is on the elevator, the elevator is at $A2$, and $A2$ is not engaged in unloading b1. By E.18, an agent other than hero can come to have b1 between SA and $S1$ only if an action "unload(b1)" occurs in an interval intersecting $[SA, S1]$. By lemma B.49, no action "do(AZ,unload(b1)" begins at an interval between $S0$ and $S1$; and by construction of SA, any action "do(AZ,unload(b1))" begun before $S0$ must be completed no later than SA. Hence, no such action occurs in an interval intersecting $[SA, S1]$.

Lemma B.51:
[AZ $\neq$hero $\wedge$ accepts_req(el2(AZ),AZ,hero,$S1$) $\wedge$ $S2 \geq S1$ $\wedge$
soc_poss($S2$) $\wedge$ time($S2$) $<$ time($S1$) + max_el2b_time] $\Rightarrow$
working_on(el2(AZ),AZ,hero,$S1, S2$).

Proof: Let SM be any situation such that $S1 \leq SM \leq S2$. Then by T.16, time(SM) $\leq$ time($S2$) $<$ time($S1$) + max_el2b_time. By lemma B.48, $\neg$terminates(el2(AZ),AZ,hero,$S1, SM$).

By QD.9, attempt_toward(el2(AZ),AZ,hero,$S1, S2$). By QD.8, since $\neg$terminates(el2(AZ),AZ,hero,$S1, SM$) for any SM between $S1$ and $S2$, it follows that begin_plan(el2(AZ),AZ,hero,$S1, S2$). By Q.5, working_on(el2(AZ),$AZ, AR, S1, S2$).

Lemma B.52:
[AZ $\neq$hero $\wedge$ accepts_req(el2(AZ),AZ,hero,$S1$) $\wedge$ $S2 \geq S1$ $\wedge$ soc_poss($S2$)] $\Rightarrow$
[working_on(el2(AZ),AZ,hero,$S1, S2$) $\Leftrightarrow$ time($S2$) $<$ time($S1$) + max_el2b_time].

Proof: The implication "working_on(el2(AZ),AZ,hero,$S1, S2$) $\Rightarrow$ time($S2$) $<$ time($S1$) + max_el2b_time" follows directly from Q.5 and Lemma B.48. The full result thus follows from B.51.

Definition BD.5: leads_towards1(E, S, I) $\equiv$ $\exists_{S2}$ occurs($E, S, S2$) $\wedge$ [$S2$ <start(I) $\vee$ elt($S2, I$)].
(There is an occurrence of event E starting in S on the same time line as u-interval I.)

Lemma B.53:
[soc_poss_int(I) $\wedge$ elt($S1, I$) $\wedge$ working_on($P, AC, AR, S0, S1$) $\wedge$ choice($A, S1$)] $\Rightarrow$
$\exists_E$ know_next_step($E, P, AC, S0, S1$) $\wedge$ leads_towards1($E, S1, I$).

Proof: From B.32, BD.4, BD.5.

Lemma B.54:
[$AZ \neq$ hero $\wedge$ working_on(el2(AZ), AZ, hero, $S0, S1$) $\wedge$ el2_q1($AZ, S1, S0$) $\wedge$ elt($S1, I$) $\wedge$ soc_poss_int(I)]
$\Rightarrow$
leads_towards1(do(AZ,call),$S1, I$)

Proof: From B.53, B.41.

Lemma B.55:
[$AZ \neq$ hero $\wedge$ working_on(el2(AZ), AZ, hero, $S0, S1$) $\wedge$ el2_q2($AZ, S1, S0$) $\wedge$
elt($S1, I$) $\wedge$ soc_poss_int(I)] $\Rightarrow$
leads_towards1(do(AZ,load(b1)),$S1, I$)

Proof: From B.54, B.42.

Lemma B.56:

$[AZ \neq$ hero $\wedge$ working_on(el2(AZ), AZ, hero, $S0, S1) \wedge$ el2_q3($AZ, S1, S0) \wedge$
elt($S1, I) \wedge$ soc_poss_int(I)$] \Rightarrow$
leads_towards1(inform(AZ,robots,loaded_since(b1, time($S0$))),$S1, I$)

Proof: From B.53, B.44.A.

Lemma B.57:
$[AZ \neq$hero $\wedge$ accepts_req(el2(AZ),AZ,hero,$S0$) $\wedge$ el2_q2($AZ, S1, S0$) $\wedge$
reserved_block(time($S1$),AZ,hero,max_action_time) $\wedge$
time($S1$) + max_action_time $\leq$ time($S0$) + max_el2b_time $\wedge$
soc_poss_int(I) $\wedge$ elt($S0, I$) $\wedge$ elt($S1, I$)$] \Rightarrow$
$\exists_{S3,S4}$ elt($S4, I$) $\wedge$ time($S3$) $\leq$ time($S1$) + max_action_time $\wedge$
leads_towards1(inform(AZ,robots,loaded_since(b1, time($S0$))),$S1, I$)

Proof: By lemma B.52, working_on(el2(AZ),AZ,hero,$S0, S1$). By lemma B.55 there exists $S2$ in I such that occurs(do(AZ,load(b1)),$S1, S2$). By M.1, time($S2$) $\leq$ time($S1$) + max_action_time $\leq$ time($S0$) + max_el2b_time. By lemma B.51, working_on(el2(AZ),AZ,hero,$S0, S2$). By E.5 and E.9 there exists SM such that $S1 < SM < S2$, holds(SM,on_elevator(b1)), and by E.8, holds(SM,elevator_at(AZ)). Thus by XD.12, holds($S2$,loaded_since(b1,AZ,time($S0$))). By lemma B.9, choice($AZ, S2$). By QD.1, reserved(time($S2$),AZ,hero). Let $S3$ be the earliest time between $S0$ and $S2$ such that holds($S3$,loaded_since(b1,AZ,time($S0$))), choice($AZ, S3$), and reserved(time($S3$),AZ,hero)). Then el2_q3($AZ, S3, S0$). The result then follows from lemma B.56.

Lemma B.58:
$[AZ \neq$hero $\wedge$ accepts_req(el2(AZ), AZ, hero,$S1$) $\wedge$ holds($S1$,has(AZ,b1)) $\wedge$ soc_poss_int($I1$) $\wedge$
elt($S1, I1$)$] \Rightarrow$
$\exists_{S2,S3,Z}$ elt($S3, I1$) $\wedge$ time($S3$) $\leq$ time($S1$) + delay_time + min_reserve_block $\wedge$
leads_towards1(inform(AZ,robots,loaded_since(b1, time($S0$))),$S1, I$).

(If, in situation $S1$, AZ has the package and AZ accepts the request el2 broadcast by the hero, then within the time max_el2_time, AZ will inform the hero that the package has been on the elevator at some time later than the broadcast.)

Proof: Let az, s1, i1 satisfy the left-hand side of the above implication.

Let t5 be the first time such that t5 $\geq$ time(s1) and reserved_block(t5,az,hero,4*max_action_time + max_elevator_wait). (The notation "4*max_action_time" here and similar notations below should be taken as syntactic sugar for "max_action_time + max_action_time + max_action_time + max_action_time". We do not have to introduce a general multiplication operator.) By Q.2 and X.7, such a t5 exists and t5 $\leq$ t1 + delay_time. Using lemma B.7, let s5 be a situation such that elt(s5,i1) and time(s5)=t5. Let s6 be the first situation after s5 in i1 such that choice(az,s6) (lemma B.13). By M.1, time(s6) $\leq$ time(s5) + max_action_time, so by lemma B.27 reserved_block(time(s6),az,hero,3*max_action_time + max_elevator_wait).

We now have a hierarchical case analysis

Case 1: Suppose that holds(s6,has(az,b1)) and $\neg$holds(s6, elevator_at(az)). Then by XD.8, holds(s6,el2_q1_f(az)), and by XD.9, el2_q1(az,s6,s6). By lemma B.54, there is a situation s7 in i1 such that occurs(do(az,call),s6,s7). Using lemma B.7, let s8 be the situation in i1 such that time(s8) = time(s7) + max_elevator_wait. Note that, by lemma B.27 and axiom M.1, reserved_block(time(s8),az,hero,2*max_action_time).

By E.4 and FD.6, there is a situation s9 in i1 such that that s7 $\leq$ s9 $\leq$ s8 and holds(s9,elevator_at(az)). We have reserved_block(time(s9),az,hero,2*max_action_time). By lemma B.13 there is a situation s10 in i1 such that choice(az,s10) within time max_action_time of time(s9). By lemma B.27 reserved_block(time(s10),az,hero,max_action_time).

Let s11 be the first situation such that s1 $\leq$ s11 $\leq$ s10, holds(s11,elevator_at(az)), choice(az,s11) and reserved_block(time(s11),az,hero,max_action_time).

There are now two cases to consider:

Case 1.1: Suppose that holds(s11,has(az,b1)). Then el2_q2(az,s11,s0), so the result follows from lemma B.57.

Case 1.2: Suppose that ¬holds(s11,has(az,b1)). Then by lemma B.43, holds(s11,loaded_since(b1,az,time(s1))). Let s12 be the first situation such that s1 < s12 $\leq$ s11, holds(s12,loaded_since(b1,az,time(s1))), choice(az,s12), and reserved(time(s12),az,hero). Then el2_q3(az,s12,s1). The result then follows from lemma B.56.

Case 2: Suppose that holds(s6,has(az,b1)) and holds(s6, elevator_at(az)). The proof continues in the same way as in case 1 from situation s9 onward.

Case 3: Suppose that ¬holds(s6,has(az,b1)). The proof continues in the same way as in case 1.2.

Lemma B.59:
[AZ $\neq$hero $\wedge$ accepts_req(el2(AZ), AZ, hero,$S1$) $\wedge$ holds($S1$,elevator_at(AZ)) $\wedge$ holds($S1$,on_elevator(b1)) $\wedge$ elt($S1, I$) $\wedge$ soc_poss_int(I)] $\Rightarrow$
$\exists_{S2,S3,Z}$ $S1 < S2 < S3 \wedge$ elt($S3, I$) $\wedge$ time($S3$) $\leq$ time($S1$) + delay_time + min_reserve_block $\wedge$ occurs(inform(AZ,robots,loaded_since(b1, time($S0$))),$S2$, $S3$).

Proof: Let az,s1,i1,s5,s6 be the same as in the proof of B.58. By XC.11, holds(s6,loaded_since(b1,az,time(s1)). The proof then continues as in Case 1.2 of lemma B.52.

Validation of Plan el1

Lemma B.60:
$\forall_{S0,S}$ $S0 < S \Rightarrow$
[[$\forall_{S0A,SA}$ [k_acc_int(hero,$S0, S, S0A, SA$) $\Rightarrow \Phi(SA, S0A)$] $\vee$
[$\forall_{S0A,SA}$ [k_acc_int(hero,$S0, S, S0A, SA$) $\Rightarrow \neg\Phi(SA, S0A)$]]
where Φ is any of the relations "el1_q1", "el1_q2a", "el1_q3", or "el1_q2".
(The hero always knows whether any of the above conditions hold.)

Proof: From lemmas B.14, B.21 together with K.3, E.19, E.21, FD.3, XD.1 through XD.5.

Lemma B.61:
el1_q1($S1, S0$) $\Rightarrow$
[know_next_step(E,el1,hero,$S1, S0$) $\Leftrightarrow$ instance(E,broadcast_req(hero,robots,r2),$S1$)] $\wedge$
[exec_cont(E,el1,hero,hero,$S1$, $S0$) $\Leftrightarrow$ instance(E,broadcast_req(hero,robots,r2),$S1$)]

Proof: By XD.2, MD.2, MD.3, $S1$ is a choice point for hero. By X.2, the only next steps of el1 in $S1$ are the instances of broadcast_req(hero,robots,r2). By lemma B.60 the hero knows that these are the only next steps for el1 in $S1$. By E.22 and Q.3, no one else governs these actions. Hence by QD.2 these are is the only executable continuation of el1 in $S1$.

Lemma B.62:
el1_q2($S1, S0$) $\Rightarrow$
[know_next_step(E,el1,hero,$S0, S0$) $\Leftrightarrow$ E=do(hero,call)] $\wedge$
[exec_cont(E,el1,hero,hero,$S1$, $S0$) $\Leftrightarrow$ E=do(hero,call)].

Proof: Analogous to lemma B.61.

Lemma B.63:

el1_q3($S1,S0$) $\Rightarrow$
[know_next_step(E,el1,hero,$S0,S0$) $\Leftrightarrow$ E=do(hero,unload(b1))] $\wedge$
[exec_cont(E,el1,hero,hero,$S1,S0$) $\Leftrightarrow$ E=do(hero,unload(b1))].

Proof: Analogous to lemma B.61.

Lemma B.64:
[working_on(el1,hero,hero,$S0,S1$) $\wedge$ elt($S1,I$) $\wedge$ soc_poss_int(I) $\wedge$ el1_q1($S1,S0$)] $\Rightarrow$
leads_towards1(broadcast_req(hero,robots,r2),$S1,I$).

Proof: From B.53, B.61.

Lemma B.65:
[working_on(el1,hero,hero,$S0,S1$) $\wedge$ elt($S1,I$) $\wedge$ soc_poss_int(I) $\wedge$ el1_q2($S1,S0$)] $\Rightarrow$
leads_towards1(do(hero,call),$S1,I$).

Proof: From B.53, B.62.

Lemma B.66:
[working_on(el1,hero,hero,$S0,S1$) $\wedge$ elt($S1,I$) $\wedge$ soc_poss_int(I) $\wedge$ el1_q3($S1,S0$)] $\Rightarrow$
leads_towards1(do(hero,unload(b1)),$S1,I$).

Proof: From B.53, B.63.

Lemma B.67:
begin_plan(el1,hero,hero,$S0,S1$) $\wedge$ terminates(el1,hero,hero,$S0,S1$) $\Rightarrow$
know_succeeds(el1,hero,$S0,S1$).
(Plan el1 can only terminates with success.)

Proof: Suppose that begin(el1,hero,hero,$S0,S1$) and $\neg$know_succeeds(el1,hero,hero,$S0,S1$). We wish to show that el1 does not terminate in $S1$. There are two cases to consider:

Case 1: $S1 = S0$ or el1_q2($S1,S0$) or el1_q3($S1,S0$). By lemmas B.61, B.62, B.63 there is an executable continuation for el1 in $S1$; hence by QD.2, QD.3, QD.5, el1 does not terminate in $S1$.

Case 2: $S1 \neq S0$ and $\neg$el1_q2($S1,S0$) and $\neg$el1_q3($S1,S0$). If $S1$ is not a choice point for the hero, then el1 does not terminate in $S1$ (QD.3, QD.4, QD.5), so assume that $S1$ is a choice point. By X.2, any action E of the hero is a next step of el1. By lemma B.60 the hero knows that $S1 \neq S0$, $\neg$el1_q2($S1,S0$), and $\neg$el1_q3($S1,S0$). so he knows that any action of his is a next step. In particular, as "wait" is always possible, he knows that "wait" is a possible next step (axioms A.7 and PD.1). Therefore, if time(s1) is reserved for hero by hero, then "Wait" is an executable continuation of el1, so abandon1 is not satisfied (QD.2, QD.3). If time(s1) is not reserved for hero by hero, then abandon2 is not satisfied (QD.4). Since, by assumption, know_succeeds is not satisfied, it follows from QD.5 that the plan does not terminate.

Lemma B.68:
el1_q1($AZ,S2,S1$) $\Rightarrow$
$\exists_E$ instance(E,broadcast_req(AZ, robots, r2), $S2$) $\wedge$ feasible($E,S2$).

Proof: By axiom E.16, it is feasible for AZ to communicate to robots. By C.5, broadcast(AZ,robots,r2) is feasible in $S2$. By C.6, know_how(AZ,broadcast(AZ,robots,r2),$S2$). The result follows from MD.1 and KHD.1.

Lemma B.69:
[working_on(el1,hero,hero,$S0,S0$) $\wedge$ elt($S0,I0$) $\wedge$ soc_poss_int($I0$) $\wedge$
$\forall_{AZ,P2}$ $AZ \neq$hero $\Rightarrow$ $\neg$working_on($P2,AZ$,hero,$S0,S0$)] $\Rightarrow$
$\exists_{SZ}$ $SZ \geq S0$ $\wedge$ elt(SZ,I) $\wedge$ completes(el1,hero,hero,$S0,SZ$).

Proof:

Assume that s0 and i0 satisfy the left hand of the implication. Let s1 be the first situation after s0 in i0 such that reserved(time(s1),hero,hero) and choice(hero,s1). By Q.2, QD.1, X.7, such an s1 will occur in i0 within time at most delay_time + max_action_time of s0. By XD.3, el1_q1(s1,s0). By lemma B.68, there is a situation s2 in i0 such that occurs(broadcast_req(hero,robots,r2),s1,s2). By S.6, the event request(hero,$A2$ assignment(r2,$A2$)) occurs from s1 to s2 for every agent $A2 \neq$hero.

By lemma B.67 and B.36, either el1 has completed before s2 or hero is still working on el1 in s2. If el1 has completed, then that completes the proof, so assume that el1 has not completed. By X.2 and lemma B.33, hero does not issue any broadcasts other than r2 between s0 and s2. By S.7, hero does not make any requests of $A2$ between s0 and s2. By Q.6, $A2$ has not accepted any other requests of hero between s0 and s2. By Q.5, $A2$ is not working on any plans of hero at s2. By Q.6, $A2$ accepts the request assignment(r2,$A2$) = el2($A2$) in s2.

By E.12, E.13 there is an agent az such that, in s2, either az has b1 or [the elevator is at az and b1 is loaded on the elevator]. By lemmas B.58, B.59 there exist situations s3, s4 in ia such that occurs(inform(az, robots, loaded_since(b1,az,time(s0))),s3,s4), and s4 in i0. By C.2, CK.1, the hero knows in s4 that a2 has informed him of this fact; that is, in every situation $S4B$ accessible from s4, it is the case that there exists an $S4B$ accessible from s4a and $S3B < S4B$ such that occurs(inform(az, robots, loaded_since(b1,az,time(s0))),$S3B$, $S4B$) By C.1, K.1, in any such $S3B$ it is the case that loaded_since(b1,az,time(s0)).

Let s5 be the first situation after s4 in i0 such that reserved_block(time(s5), hero, hero, 3*max_action_time + max_elevator_wait). By Q.2, X.7, time(s5) $\leq$ time(s4) + delay_time. Suppose that k_acc(hero,s5,$S5B$) accessible from s5. By K.4, there exists $S4B \leq S5B$ such that k_acc(hero,s4,$S4B$). By lemma B.50, b1 is on the elevator in $S5B$. Thus by XD.1 holds(s5, know_loaded(hero,b1)). Let s6 be the first opportunity after s0 in which know_loaded(hero,b1); then time(s6) $\leq$ time(s5) + max_action_time and reserved_block(time(s6), hero, hero, 2*max_action_time + max_elevator_wait).

There are now two cases to consider:

Case 1: Suppose that el1_q3(S,s0) does not hold for any S between s0 and s6. Then el1_q2(s6,s0) (XD.4, XD.5). By lemma B.62 there exists s7 in i0 such that occurs(do(hero,call),s6,s7). Using E.4, FD.6, let s8 be the first situation in i0 such that time(s8) $\leq$ time(s7) + max_elevator_wait $\leq$ time(s6) + max_action_time + max_elevator_wait and holds(s8, elevator_at(hero)). Let s9 be the first choice point for hero in i0 after s8; thus time(s9) $\leq$ time(s8) + max_action_time. By E.7, E.1, the elevator is still at the hero in s9; by B.50 package b1 is still on the elevator in s9; and time(s9) is still reserved by the hero for himself. Let s10 be the first choice point in i0 after s0 such that in s10 the elevator is at the hero, the package is on the elevator and the time is reserved by the hero for himself. Then el1_q3(s10,s0). By Q.2, time(s10) $\leq$ time(s9) + delay_time. By lemma B.66, occurs(do(hero,unload(b1)),s10,s11) for some s11 in i0. Thus s11 satisfies the right hand side of the implication.

Case 2: Suppose that el1_q3(S,s0) holds for some S between s0 and s6. Then the proof continues as in Case 1, from s10 on.

▮

Lemma B.70: k_acc(hero,s0,$S0A$) $\Rightarrow$ executable(el1,hero,$S0A$)

Proof: Assume that k_acc(hero,s0,s0a), occurs(do(hero,commit(hero,el1)),s0a,s1a), elt(s1a,i0), and soc_poss_int(i0). By X.13 $\neg\exists_{P,AC,SX}$ working_on(P, AC,hero,SX,s0a); that is, in s0a no one including hero is working on any plans of hero's. Since no other commit or broadcast actions occur between s0a and s1a (axioms A.1, A.2), no other requests occur (S.7) or are accepted (Q.6); hence, in s1a still no one is working on any plans of hero's (lemma B.31). By lemma B.69, el1 completes in i0. Therefore, el1 is executable in s0a (Q.11).

Theorem B.71: know_achievable(has(hero,b1),el1,hero,s0).

Proof: From lemma B.70 we have k_acc(hero,s0,$S0A$) $\Rightarrow$ executable(el1,hero,$S0A$). From X.1, QD.8, PD.2, K.1, we have completes(el1,hero,hero,$S0A, S1A$) $\Rightarrow$ holds($S1A$,has(hero,b1)). The result follows from QD.16. ∎