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 $S_1$ is a successor of $S_0$, denoted “$\text{succ}(S_1, S_0)$” if $S_1$ follows immediately after $S_0$.

$$\text{succ}(S_1, S_0) \equiv S_0 < S_1 \land \neg \exists S \; S_0 < S < S_1.$$  

Lemma B.1: $\text{succ}(S_1, S_0) \leftrightarrow \text{time}(S_1) = \text{time}(S_0) + 1 \land S_1 > S_0$. 

* The research reported in this paper was supported in part by NSF grant IIS-0097537.
Lemma B.5: (Induction from situations to intervals: Schema) Let $\phi$ be a formula with an open situation variable $S$. Assume that the variable $SF$ does not appear free in $\phi$. Then the closure of the following formula holds:

$$\exists S \exists I, S < I \land \forall S, S \leq I \land \phi(I) \Rightarrow \phi(S).$$

Proof: Assume that the left hand of the implication holds for some $s_0$. Let $\Gamma(S)$ be the formula, open in $S$, $\forall S, s_0 \leq S \leq I \Rightarrow \phi(S)$. Then by assumption $\Gamma(s_0)$ and $\vee S, \Gamma(S) \Rightarrow \exists S, S > S \land \Gamma(S)$. From axiom I.5, it follows that there exists a u-interval $i_0$ starting in $s_0$ in which $\Gamma$ holds infinitely often; i.e.

$$s_0 = \text{start}(i_0) \land \forall S, \text{elt}(S,i_0) \Rightarrow \exists S_2, S < S_2 \land \Gamma(S_2) \land \text{elt}(S_2,i_0).$$

Now, lest $sa$ be any situation in $i_0$. We have shown that $\exists S_2, sa < S_2 \land \Gamma(S_2)$; but, by definition of $\Gamma$, that means that $\phi(sa)$.

Lemma B.6: (Existence of a “first” situation after $S_0$ satisfying $\phi$.) (Schema) Let $\phi(S)$ be a formula with an open situation variable $S$. Assume that the variable $SF$ does not appear free in $\phi$. Then the closure of the following formula holds:

$$\phi(S_1) \land s_0 < S_1 \Rightarrow \exists S, \phi(SF) \land S_0 \leq SF \land \forall S, S_0 \leq S \land SF \Rightarrow \neg \phi(S).$$

Proof: Assume that $S_0 < S_1$ and $\phi(S_1)$. For any duration $D$, let $\Gamma(D)$ be the formula,

$$\exists S, \text{time}(SD) = \text{time}(S_0) + D \land S_0 \leq SD \leq S_1 \land \phi(SD).$$

By assumption $\Gamma(D1)$ holds for $D1 = \text{time}(S1) - \text{time}(S)$. Hence there is some smallest positive value $DF$ such that $\Gamma(DF)$. By construction of $\Gamma$, there exists an $SF$ such that $\text{time}(SF) = DF$, $S_0 \leq SF$
and \( \phi(SF) \). Let \( S \) be any situation such that \( S_0 \leq S < SF \), and let \( D = \text{time}(S) - \text{time}(S_0) \). Since \( D < DF \), we must have \( -\Gamma(D) \). Since \( S_0 \leq S < S_1 \), we must have \( -\phi(SD) \).

**Lemma B.7:** If \( i_0 \) be an interval, let \( s_0 = \text{start}(i_0) \), and let \( t_0 = \text{time}(s_0) \). Let \( \Phi(D) \) be the formula "\( \exists_{S_1} \text{time}(S)=t_0 + D \wedge \text{elt}(S,i_0)\)". Clearly, since \( \text{elt}(s_0,i_0) \), it follows that \( \Phi(0) \). Suppose, inductively, that \( D_1 \geq 0 \) and \( \Phi(D_1) \). Then there exists a situation \( S_X \) such that \( \text{time}(S_X)=t_0+D_1 \) and \( \text{elt}(S_X,i_0) \). Let \( S_L \) be any successor to \( S_X \). By A.4, there exists a situation \( S_2 \) such that \( \neg(S_2 < S_1) \) and \( \text{elt}(S_2,i_0) \). By T.18, there exists a situation \( S_M \) such that \( \text{time}(S_M)=t_0+D+1 \) and \( \text{ordered}(S_M,S_2) \). Using T.16, it follows that in fact \( S_X < S_M \leq S_2 \), so by I.2, \( \text{elt}(S_M,i_0) \). Thus \( \Phi(D_1 + 1) \). 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:**
\[ \text{action}(E_1, A) \wedge \text{action}(E_2, A) \wedge \text{leads_toward}(E_1, S_0, S_1) \wedge \text{leads_toward}(E_2, S_0, S_2) \wedge \text{ordered}(S_1, S_2) \] \[ \Rightarrow E_1 = E_2. \]

**Proof:** Immediate from A.1, EVD.1, AD.2, when \( \text{time}(S_0) > 0t \); from A.6, AD.3 when \( \text{time}(S_0) = 0t \).

**Lemma B.9:**
\[ \text{action}(E, A) \wedge \text{occurs}(E, S_1, S_2) \Rightarrow \text{choice}(A, S_2). \]

**Proof:** From A.2, AD.3.

**Lemma B.10:**
\[ S_0 < S_1 < S_2 \wedge S_1 < S_X \wedge \text{occurs}(E, S_0, S_2) \wedge \text{action}(E, A) \Rightarrow \exists_{S_Y} \text{ ordered}(S_X, S_Y) \wedge \text{occurs}(E, S_0, S_Y). \]

(If \( S_1 \) is in the middle of the execution of \( E \) (between \( S_0 \) and \( S_2 \)) then this execution is completed along every time line that contains \( S_1 \).)

**Proof:** By EVD.1 \text{ leads_towards}(E, S_0, S_1). By axiom A.1, \( \exists_{E_1} \text{ action}(E_1, A) \wedge \text{leads_toward}(E_1, S_0, S_X) \). By EVD.1, there exists \( S_Y \) such that \( \text{occurs}(E_1, S_0, S_Y) \) and \( \text{ordered}(S_Y, S_X) \). By lemma B.3, \( \text{ordered}(S_Y, S_1) \). By EVD.1, \text{ leads_towards}(E_1, S_0, S_1). But by A.1, the action of \( A \) that leads from \( S_0 \) toward \( S_1 \) is unique; hence \( E_1 = E \).

**Lemma B.11:**
\[ \forall_{A, S_0, S_2} S_0 < S_2 \Rightarrow \exists_{S_X, S_Y} S_X < S_0 < S_Y \wedge \text{action}(E, A) \wedge \text{occurs}(E, S_X, S_Y) \wedge \text{ordered}(S_Y, S_2). \]

(Any situation \( S_0 \) occurs either at the beginning or in the middle of an action \( E \) that starts in \( S_X \) before or at \( S_0 \), and that continues along every time line (toward \( S_2 \)) containing \( S_0 \).)

**Proof:** If choice\((A, S_0)\) then choose \( S_X = S_0 \). By axiom A.1 there exists an action \( E \) of \( A \) such that \text{leads_toward}(E, S_0, S_2); that is, by EVD.1, there exists \( S_Y \) such that \text{ordered}(S_Y, S_2) and \text{occurs}(E_1, S_0, S_Y).

Otherwise, if not choice\((A, S_0)\), then by AD.3 and AD.1 there exists \( S_X, S_Z, E \) such that action\((E, A)\), \( S_X < S_0 < S_Z \) and \text{occurs}(E, S_X, S_Z). The result then follows from lemma B.10.

**Lemma B.12:**
\[ \forall_{A, S_0, S_2} S_0 < S_2 \Rightarrow \exists_{S_Y} \text{ choice}(A, S_Y) \wedge S_0 < S_Y \wedge \text{ordered}(S_Y, S_2) \wedge \text{time}(S_Y) \leq \text{time}(S_0) + \max_{\text{action_time}}. \]

(On any time line, choice points for \( A \) occurs with a maximum gap of \( \max_{\text{action_time}} \).)

**Proof:** By lemma B.11, there exist \( E, S_X, S_Y \) such that action\((E, A)\), \text{occurs}(E, S_X, S_Y), \( S_X \leq S_0 < S_Y \) and \text{ordered}(S_Y, S_2). By M.1, \text{time}(S_Y) \leq \text{time}(S_X) + \max_{\text{action_time}} \leq \text{time}(S_0) +
Lemma B.13:
elt(S, I) ⇒
\[\exists s_1 \ S < s_1 \land \elt(S, I) \land \\text{choice}(A, S_1) \land \text{time}(S_1) \leq \text{time}(S) + \max \text{action_time}.\]

Proof: By lemma B.7, there exists S2 in I such that time(S2) = time(S) + max action_time. The result then follows from B.12.

Lemma B.14: \(k_{\text{acc}}(A, S_0, S_0A) \Rightarrow \text{time}(S_0) = \text{time}(S_0A)\).

Proof by contradiction. Suppose this is false. Since \(k_{\text{acc}}\) is symmetric by axiom K.3, there exists \(A, S_0, S_0A\) for which \(k_{\text{acc}}(A, S_0, S_0A)\) and \(\text{time}(S_0) < \text{time}(S_0A)\). Let \(t_1\) be the earliest time for which there exists \(a, s_1, s_1a\) such that \(k_{\text{acc}}(a, s_1, s_1a)\) and \(t_1 = \text{time}(s_1) < \text{time}(s_1a)\). Using T.18, choose an \(a, s_a\) such that \(\text{time}(s_a) = t_1, s_a < s_1a\). Using K.3, K.4 there exists a situation \(s\) such that \(k_{\text{acc}}(a, s, s)\), \(s < s_1\). By T.16, \(\text{time}(s) < \text{time}(s_1)\). But then, by K.3, we have \(k_{\text{acc}}(a, s, s_a)\) and \(\text{time}(s) < \text{time}(s_a) = t_1\), contradicting the assumption that \(t_0\) was the earliest time when this could happen.

Lemma B.15: \(k_{\text{acc}}(A, SXA, SXB) \land \text{occurs}(E, SXA, SYA) \land \text{action}(E, A) \Rightarrow \exists SYB \ \text{occurs}(E, SXB, SYB)\).

Proof: By K.5, there exists \(S1B, S2B\) such that \(k_{\text{acc}}(A, SXA, S1B), S1B \leq SXB\), and \(\text{occurs}(E, S1B, S2B)\). (Bind \(S1A\) in K.5 to \(SX\) here; \(S2A\) to \(SY\); \(SA\) to \(SX\) and \(S2B\) to \(SY\).) 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: \(\text{choice}(A, S_1) \land k_{\text{acc}}(A, S_1, S1A) \Rightarrow \text{choice}(A, S1A)\).

(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 choice(A, S1A).

Lemma B.17: \(\forall_{SA} k_{\text{acc}}(A, S, SA) \Rightarrow \text{choice}(A, SA)) \lor [\forall_{SA} k_{\text{acc}}(A, S, SA) \Rightarrow \neg \text{choice}(A, SA)]\).

(You know whether you’re at a choice point.)

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

Lemma B.18:
\[\text{action}(E, A) \land k_{\text{acc}}(A, S0, S0A) \land \text{feasible}(E, S0) \Rightarrow \text{feasible}(E, S0A)\].

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:
\[k_{\text{acc}}(A, S, SA) \land \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: \(\text{know}_{\text{whether}}(A, Q, S) \equiv [\forall_{SA} k_{\text{acc}}(A, S, SA) \Rightarrow \text{holds}(SA, Q)] \lor [\forall_{SA} k_{\text{acc}}(A, S, SA) \Rightarrow \neg \text{holds}(SA, Q)]\)

(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:
\(k_{\text{acc_int}}(A, S1, S1A, S2A) \equiv k_{\text{acc}}(A, S1, S1A) \land k_{\text{acc}}(A, S2, S2A) \land S1 < S2 \land S1A < S2A\).

(Interval \([S1A, S2A]\) is knowledge accessible from \([S1, S2]\).
Lemma B.20:
\[ \forall S \text{ know whether}(AC, Q, S) \Rightarrow \]
\[ \forall S_0, S_1 \text{ } [k_{\text{acc int}}(AC, S_0, S_1, S_0A, S_1A) \Rightarrow \text{opportunity}(S_1A, AC, AR, Q)] \lor \]
\[ \forall S_0, S_1 \text{ } [k_{\text{acc int}}(AC, S_0, S_1, S_0A, S_1A) \Rightarrow \neg \text{opportunity}(S_1A, AC, AR, Q)] \]
(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:
\[ \forall S \text{ know whether}(AC, Q, S) \Rightarrow \]
\[ \forall S_0, S_1 \text{ } [k_{\text{acc int}}(AC, S_0, S_1, S_0A, S_1A) \Rightarrow \text{first opportunity}(S_1A, AC, AR, S_0A, Q)] \lor \]
\[ \forall S_0, S_1 \text{ } [k_{\text{acc int}}(AC, S_0, S_1, S_0A, S_1A) \Rightarrow \neg \text{first opportunity}(S_1A, AC, AR, S_0A, Q)] \]
(If AC always knows whether Q is true, then he always know whether S1 is the first opportunity to act on Q.)


Lemmas about plans

Lemma B.22: begin plan(P, AC, AR, S0, S1) \land S0 ≤ SM < S1 ⇒ begin plan(P, AC, AR, S0, SM).

Proof: From QD.6

Lemma B.23:
attempt toward(P, AC, AR, S0, S1) \land S0 ≤ SM < S1 ⇒ 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:
[begin plan(P, AC, AR, S0, S1) \land choice(AC, S1) \land \neg terminates(P, AC, AR, S0, S1) \land know next step(E, P, AC, S0, S1) \land leads towards(E, S1, S2) \land succ(S2, S1)] ⇒ 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 begin plan(P . . . S2) recursively in terms of begin plan(P . . . S1) where S1 is the predecessor of S2.

Assume that the left-hand side of the above implication holds. By QD.6, since begin plan(P, AC, AR, S0, S1) we have S0 ≤ S1. Since 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

\[ \neg \text{terminates}(P, AC, AR, S0, SM) \land \]
\[
\text{choice}(AC, SM) \Rightarrow \exists E \: \text{know\_next\_step}(E, P, AC, S0, SM) \land \text{leads\_towards}(E, SM, SZ)
\]

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:**

\[
\text{begin\_plan}(P, AC, AR, S0, S1) \land \neg\text{choice}(AC, S1) \land 
\neg\text{know\_succeeds}(P, AC, S0, S1) \land \text{succ}(S2, S1) \Rightarrow 
\text{begin\_plan}(P, AC, AR, S0, S2).
\]

**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:**

\[
\text{begin\_plan}(P, AC, AR, S0, S1) \land S0 \leq SM < S1 \land \text{leads\_towards}(E, SM, S1) \land \text{action}(E, AC) \Rightarrow 
\text{know\_next\_step}(E, P, AC, S0, SM).
\]

**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:** \(\forall S1, S2 \: S1 < S2 \land \text{soc\_poss}(S2) \Rightarrow \text{soc\_poss}(S1)\).

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

**Lemma B.27:**

\[
[D1 \geq 0 \land D2 \geq 0 \land T \leq T2 \leq T + D1 \land \text{reserved\_block}(T, AC, AR, D1 + D2)] \Rightarrow 
\text{reserved\_block}(T2, AC, AR, D2)
\]

**Proof:** From QD.1 with arithmetic.

**Lemma B.28:** \(\text{working\_on}(P, AC, AR, S0, S1) \land S0 \leq SB \leq S1 \Rightarrow \text{working\_on}(P, AC, AR, S0, SB)\).

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

**Lemma B.29:**

\[
\text{working\_on}(PX, AC, AR, SX, S) \land \text{working\_on}(PY, AC, AR, SY, S) \Rightarrow PY = PX \land SY = SX.
\]

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\(_\text{on}(P X, AC, AR, SX, SY)\). By Q.6 since accepts\(\text{req}(PY, AC, AR, SY)\), it follows that \(\forall\_PQ, SQ\text{ working}_{\text{on}}(PQ, AC, AR, SQ, SY) \Rightarrow PQ = PY, SQ = SX\). Hence \(P X = PY, SX = SY\).

**Lemma B.30**
\([\text{working}_{\text{on}}(P, AC, AR, S 0, S 1) \land \text{action}(E, AC) \land S 0 \leq SM \land \text{leads\_toward}(E, SM, S 1)] \Rightarrow \text{know\_next\_step}(E, P, AC, S 0, SM)\).

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

**Lemma B.31**
\([-\exists S 0 \text{ working}_{\text{on}}(P, AC, AR, S 0, S 1)] \land \text{working}_{\text{on}}(P, AC, AR, S 2, S 3) \land S 1 < S 3 \Rightarrow S 1 < S 2 \land \exists S X \text{ occurs(request}(AC, AR, P), SX, S 2)\).

(If AC goes from not working on P in S 1 to working on P from S 2 to S 3, then a request to do P must have completed at S 2.)

**Proof:** Since working\(_{\text{on}}(P, AC, AR, S 2, S 3)\), by Q.5 accepts\(\text{req}(P, AC, AR, S 2)\). By lemma B.28, for all SB between S 2 and S 3, working\(_{\text{on}}(P, AC, AR, S 2, SB)\). Hence S 1 is not between S 2 and S 3, so S 1 < S 2. By Q.6 there exists an SX such that occurs(request\((P, AC, AR), SX, S 2)\).

**Definition BD.4:**
\[\text{good\_action}(E, AC, S 1) \equiv \text{choice}(AC, S 1) \land \forall\_P, A R, S 0 [\text{working}_{\text{on}}(P, AC, AR, S 0, S 1) \Rightarrow \text{know\_next\_step}(E, P, AC, AR, S 0, S 1)]\].

Action\(E\) is a good action for\(AC\) in S 1 if it is a continuation of every plan\(P\) that\(AC\) is currently working on.

**Lemma B.32:** \(\forall\_AC, S \text{ choice}(AC, S) \Rightarrow \exists E \text{ good\_action}(E, AC, S)\).

“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\(AR, P, S 0\) such that\(AC\) reserves\(time(S)\) for\(AR\) and working\(_{\text{on}}(P, AC, AR, S 0, S)\).

By axiom Q.1 and lemma B.29 there is at most one such\(AR, P,\) and\(S 0\).

Case 1.1 : Suppose there is an action\(E\) such that exec\(_{\text{cont}}(E, P, AC, AR, S 0, S)\).

By QD.2, know\(_{\text{next\_step}}(E, P, AC, AR, S 0, S)\). Let\(P X \neq P, ARX, S 0X\) be any values such that working\(_{\text{on}}(P X, AC, ARX, S 0X, S)\). By lemma B.29,\(ARX \neq AR\), so by Q.1, \(\neg\text{reserved}(time(S), AC, ARX)\). By QD.2 \(\neg\text{governs}(ARX, E)\) and by PD.1 feasible\((E, S)\).

Since working\(_{\text{on}}(P X, AC, ARX, S 0X, S)\), by Q.5 \(\neg\text{terminates}(P X, AC, ARX, S 0X, S)\).

By QD.5 \(\neg\text{abandon2}(P, AC, ARX, S 0X, S)\). By QD.4, for any action\(E 1\), if action\((E 1, AC)\) and \(\neg\text{governs}(ARX, E 1)\) then know\(_{\text{next\_step}}(E 1, P, AC, S 0X, S)\). In particular know\(_{\text{next\_step}}(E, P, AC, S 0X, S)\).

Since the implication “working\(_{\text{on}}(P X, AC, ARX, S 0X, S) \Rightarrow \text{know\_next\_step}(E, P X, AC, S 0X, S)\)” holds for all\(PX, ARX, S 0X, S\), we have good\(_{\text{action}}(E, AC, S)\) (definition BD.4).

Case 1.2 Suppose that there is no action\(E\) such that exec\(_{\text{cont}}(E, P, AC, AR, S 0, S)\). By QD.3, abandon1\((P, AC, AR, S 0, S)\). By QD.5, terminates\((P, AC, AR, S 0, S)\). But by Q.5 this contradicts the assumption that working\(_{\text{on}}(P, AC, AR, S 0, S)\).

Case 2. Suppose that\(\text{reserved}(time(S), AC, AR)\) and choice\((AC, S)\), but there is no plan\(P\) and situation\(S 0\) such that working\(_{\text{on}}(P, AC, AR, S 0, S)\). Let\(E = \text{do}(AC, \text{wait})\), so\(E\) is not governed by any agent (Q.4). Let\(P X, ARX, S 0X\) be any values such that working\(_{\text{on}}(P X, AC, ARX, S 0X, S)\).

Then we can prove that\(\text{know\_next\_step}(E, P X, AC, S 0X, S)\) 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$(AC, \text{wait})$, 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$_{poss}(S1) \land S < S1 \land$ leads$_{towards}(E, S, S1) \land$ 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,

\[ \text{choice}(AC, S) \land \forall_{P,AR,S0} \text{working}_{on}(P, AC, AR, S0, S) \Rightarrow \text{know}_{next\_step}(E, P, AC, S0, S) \]

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$_{req}(P, AC, AR, S0)$ 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 $\forall_{SM} S0 \leq SM < S \Rightarrow$ 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 suc$(S4, S)$ 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:**

\[ [\forall_{S,AC,E} [S < S1 \land action(E, AC) \land leads_{towards}(E, S, S1)] \Rightarrow good_{action}(E, AC, S)]] \Rightarrow soc_{poss}(S1) \]

(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$_{poss}(S1) \iff$

\[ [\forall_{S,AC,E} [S < S1 \land action(E, AC) \land leads_{towards}(E, S, S1)] \Rightarrow good_{action}(E, AC, S)]] \]

($S1$ is socially possible if and only if all actions before $S1$ are good.)

**Proof:** From B.33 and B.34.

**Lemma B.36:**

\[ \text{accepts}_{req}(P, AC, AR, S0) \land S1 > S0 \land \text{soc}_{poss}(S1) \Rightarrow \text{working}_{on}(P, AC, AR, S0, S1) \lor \]

\[ \text{working}_{on}(P, AC, AR, S0, S1) \lor \]
\[\exists SM \ 0 \leq SM \leq S1 \land \begin{array}{l}
\text{plan}(P, AC, AR, S0, SM) \\
\text{\& terminates}(P, AC, AR, S0, SM)
\end{array}\]

**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:** \(soc\_poss(S0) \Rightarrow \exists S1 \ soc\_succ(S1, S0) \land soc\_poss(S1)\).

**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 \(soc\_poss(S1, S)\). If \(S\) is not a choice point for any agent \(A\), let \(S1\) be any situation such that \(soc\_poss(S1, S)\). 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** \(soc\_poss(S) \Rightarrow \exists I \ S=start(I) \land soc\_poss\_int(I)\). (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:** \(k\_acc(A, S1, S1A) \land T0 < time(S1) \Rightarrow holds(S1, loaded\_since(B, A, T0)) \iff holds(S1A, loaded\_since(B, A, T0))\).

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

**Lemma B.40:**

\[
\begin{align*}
\forall S0&A,S,A & k\_acc\_int(A, S0, S, S0A, SA) \Rightarrow \Phi(A, SAF, S0A) \\
\forall S0&A,S,A & k\_acc\_int(A, S0, S, S0A, SA) \Rightarrow \neg \Phi(A, SAF, S0A)
\end{align*}
\]

where \(\Phi\) is any of \((el2\_A1)\), \((el2\_A1)\), \((el2\_A2)\), \((el2\_A3)\), and \((el2\_A3)\).

(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:**

\[(AZ \neq \text{hero} \land el2\_A1(AZ, S2, S1)) \Rightarrow \\
\begin{array}{l}
[\text{know\_next\_step}(E, el2(AZ), AZ, S2, S1) \iff E=do(AZ, \text{call})]
\end{array}\]

**Proof:** By X.6, the only next step of \(el2(AZ)\) in \(S2\) is \(do(AZ, \text{call})\). 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:**

\[(AZ \neq \text{hero} \land el2\_A2(AZ, S2, S1)) \Rightarrow \\
[\text{know\_next\_step}(E, el2(AZ), AZ, S2, S1) \iff E=do(AZ, \text{load(b1)})]\]

**Proof:** Analogous to lemma B.41.

**Lemma B.43:**

\[(\exists S3, S4 \text{ such that } S3 < S2, S1 < S4, \text{ ordered}(S2, S4) \text{ and occurs}(do(AZ, \text{load(B)}), S3, S4)).
\]

**Proof:** By E.17 there exist \(S3, S4\) such that \(S3 < S2, S1 < S4, \text{ ordered}(S2, S4)\) and \(\text{occurs}(do(AZ, \text{load(B)}), S3, S4)\). By E.5 there exists \(SM < S4\) such that \(\text{throughout}(SM, S4, \text{on\_elevator(B)})\). Let \(SA\) be the earlier of \(SM, S2\); thus \(SA < S4\) and \(SA \leq S2\). By E.9, holds(\(SA\), \text{elevator\_init}(AZ)). Hence, by XD.10,
Lemma B.44:
\[ AZ \neq \text{hero} \land \text{el2}_q(AX, S2, S1) \implies [\text{know\_next\_step}(E, \text{el2}(AZ), AZ, S2, S1) \iff \text{instance}(E, \text{inform}(AZ, \text{robots}, \text{loaded\_since}(b1, AZ, \text{time}(S1)), S2))] \]

**Proof:** Analogous to lemma B.41.

Lemma B.44.A:
\[ \text{el2}_q(AX, S2, S1) \implies \exists_{E} \text{instance}(E, \text{inform}(AZ, \text{robots}, \text{loaded\_since}(b1, AZ, \text{time}(S1)), S2)) \land \text{feasible}(E, S2). \]

**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:
\[ AZ \neq \text{hero} \land \text{choice}(AZ, S1) \land \neg \text{el2}_q(AX, S2, S1) \land \neg \text{el2}_q(AX, S2, S1) \land \neg \text{el2}_q(AX, S2, S1) \implies [\text{next\_step}(E, \text{el2}(AZ), S1, S2) \iff [\text{action}(E, AZ) \land E \neq \text{do}(AZ, \text{unload}(b1))]. \]

**Proof:** From X.6.

Lemma B.46:
\[ AZ \neq \text{hero} \land \text{choice}(AZ, S1) \land \neg \text{el2}_q(AX, S2, S1) \land \neg \text{el2}_q(AX, S2, S1) \land \neg \text{el2}_q(AX, S2, S1) \implies [\text{know\_next\_step}(E, \text{el2}(AZ), AZ, S1, S2) \iff [\text{action}(E, AZ) \land E \neq \text{do}(AZ, \text{unload}(b1)) \land \text{feasible}(E, S2)]. \]

**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: \( \neg \text{abandon2}(\text{el2}(AZ), AZ, \text{hero}, S1, S2) \)

**Proof:** By QD.4, if reserved(time(S2), AZ, hero), then \( \neg \text{abandon2}(\text{el2}(AZ), AZ, \text{hero}, S1, S2) \). Suppose that \( \neg \text{reserved}(\text{time}(S2), AZ, \text{hero}) \). By MD.2, MD.3, XD.7, XD.9, XD.11, none of the conditions el2_q1(AX, S1, S2), el2_q2(AX, S1, S2), el2_q3(AX, 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(AX, S1A, S2A), el2_q2(AX, S1A, S2A), el2_q3(AX, 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:
\[ \text{terminates}(\text{el2}(AZ), AZ, \text{hero}, S1, S2) \iff S2 > S1 \land \text{time}(S2) \geq \text{time}(S1) + \text{max}_{\text{el2b\_time}}. \]

**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) \( \geq \text{time}(S1) + \text{max}_{\text{el2b\_time}}. \)

Lemma B.49:
\[ AZ \neq \text{hero} \land \text{working\_on}(\text{el2}(AZ), AZ, \text{hero}, S0, S1) \implies \neg \exists_{S2} S0 \leq S2 < S1 \land \text{leads\_toward}(\text{do}(AZ, \text{unload}(b1)), S2, S1). \]
Lemma B.50:
\[ \text{holds(S1, loaded\(\text{since}(b1,A2,\text{time}(S0))) \land} \]
\[ \forall_AZ_AZ \neq \text{hero} \Rightarrow \text{working\(\text{on}(el2(AZ),AZ,\text{hero},S0,S1))] \Rightarrow \]
holds(S1,\text{on\(\text{elevator}(b1)) \lor \text{holds}(S1,\text{has\(\text{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:
\[ AZ \neq \text{hero} \land \text{accepts\_req(el2}(AZ),AZ,\text{hero},S1) \land S2 \geq S1 \land \text{soc\_poss(S2)} \land \text{time}(S2) < \text{time}(S1) + \text{max}\_\text{el2b\_time} \Rightarrow \]
working\(\text{on}(el2(AZ),AZ,\text{hero},S1,S2)).

Proof: Let SM be any situation such that S1 ≤ SM ≤ S2. Then by T.16, \text{time(SM)} ≤ \text{time(S2)} < \text{time(S1) + max}\_\text{el2b\_time}. By lemma B.48, \text{\neg terminates(el2(AZ),AZ,hero,S1,SM)}.

By QD.9, \text{attentt\_toward}(el2(AZ),AZ,\text{hero},S1,S2). By QD.8, since \text{\neg terminates(el2(AZ),AZ,hero,S1,SM)} for any SM between S1 and S2, it follows that begin\_\text{plan(el2(AZ),AZ,hero,S1,S2).} By Q.5, working\(\text{on}(el2(AZ),AZ,AR,S1,S2).)

Lemma B.52:
\[ AZ \neq \text{hero} \land \text{accepts\_req(el2}(AZ),AZ,\text{hero},S1) \land S2 \geq S1 \land \text{soc\_poss(S2)} \Rightarrow \]
working\(\text{on}(el2(AZ),AZ,\text{hero},S1,S2) \Leftrightarrow \text{time}(S2) < \text{time}(S1) + \text{max}\_\text{el2b\_time}. \]

Proof: The implication “working\(\text{on}(el2(AZ),AZ,\text{hero},S1,S2) \Rightarrow \text{time}(S2) < \text{time}(S1) + \text{max}\_\text{el2b\_time}” follows directly from Q.5 and Lemma B.48. The full result thus follows from B.51.

Definition BD.5: \text{leads\_towards1}(E,S,I) = \exists_{S2} \text{occurs}(E,S,S2) \land [S2 < start(I) \lor 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:
\[ \text{soc\_poss\_int}(I) \land elt(S1,I) \land working\(\text{on}(P,AC,AR,S0,S1) \land choice(A,S1)) \Rightarrow \]
\[ \exists_E \text{know\_next\_step}(E,P,AC,S0,S1) \land \text{leads\_towards1}(E,S1,I). \]

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

Lemma B.54:
\[ AZ \neq \text{hero} \land working\(\text{on}(el2(AZ),AZ,\text{hero},S0,S1) \land el2\_q1(AZ,S1,S0) \land elt(S1,I) \land \text{soc\_poss\_int}(I)] \Rightarrow \]
\text{leads\_towards1}(\text{do}(AZ,\text{call}),S1,I)

Proof: From B.53, B.41.

Lemma B.55:
\[ AZ \neq \text{hero} \land working\(\text{on}(el2(AZ),AZ,\text{hero},S0,S1) \land el2\_q2(AZ,S1,S0) \land elt(S1,I) \land \text{soc\_poss\_int}(I)] \Rightarrow \]
\text{leads\_towards1}(\text{do}(AZ,\text{load}(b1)),S1,I)

Proof: From B.54, B.42.

Lemma B.56:
[AZ \neq \text{hero} \land \text{working\_on}(el2(AZ), AZ, \text{hero}, S0, S1) \land el2\_q3(AZ, S1, S0) \land elt(S1, I) \land \text{soc\_pos\_int}(I)] \Rightarrow 
\text{leads\_towards\_1(inform(AZ, robots, \text{loaded\_since}(b1, \text{time}(S0))), S1, I)}

\textbf{Proof:} From B.53, B.44.A.

\textbf{Lemma B.57:}

\[ AZ \neq \text{hero} \land \text{accepts\_req}(el2(AZ), AZ, \text{hero}, S0) \land el2\_q2(AZ, S1, S0) \land 
\text{reserved\_block}(\text{time}(S1), AZ, \text{hero}, \text{max\_action\_time}) \land 
\text{time}(S1) + \text{max\_action\_time} \leq \text{time}(S0) + \text{max\_el2\_b\_time} \land 
\text{soc\_pos\_int}(I) \land \text{elt}(S0, I) \land \text{elt}(S1, I)] \Rightarrow 
\exists S3, S4 \text{ elt}(S4, I) \land \text{time}(S3) \leq \text{time}(S1) + \text{max\_action\_time} \land 
\text{leads\_towards\_1(inform(AZ, robots, \text{loaded\_since}(b1, \text{time}(S0))), S1, I)}

\textbf{Proof:} By lemma B.52, working\_on(el2(AZ), AZ, \text{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 \text{time}(S1) + \text{max\_action\_time} \leq \text{time}(S0) + \text{max\_el2\_b\_time}. By lemma B.51, working\_on(el2(AZ), AZ, \text{hero}, S0, S2). By E.5 and E.9 there exists SM such that S1 < SM < S2, holds(SM, \text{on\_elevator}(b1)), and by E.8, holds(SM, \text{elevator\_at}(AZ)). Thus by XD.12, holds(S2, \text{loaded\_since}(b1, AZ, \text{time}(S0))). By lemma B.9, choice(AZ, S2). By QD.1, reserved(time(S2), AZ, \text{hero}). Let S3 be the earliest time between S0 and S2 such that holds(S3, \text{loaded\_since}(b1, AZ, \text{time}(S0))), choice(AZ, S3), and reserved(time(S3), AZ, \text{hero}). Then el2\_q3(AZ, S3, S0). The result then follows from lemma B.56.

\textbf{Lemma B.58:}

\[ AZ \neq \text{hero} \land \text{accepts\_req}(el2(AZ), AZ, \text{hero}, S1) \land \text{holds}(S1, \text{has}(az, b1)) \land \text{soc\_pos\_int}(I1) \land 
\text{elt}(S1, I1)] \Rightarrow 
\exists S2, S3, Z \text{ elt}(S3, I1) \land \text{time}(S3) \leq \text{time}(S1) + \text{delay\_time} + \text{min\_reserve\_block} \land 
\text{leads\_towards\_1(inform(AZ, robots, \text{loaded\_since}(b1, \text{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.)

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

Let t5 be the first time such that t5 \geq \text{time}(s1) and reserved\_block(t5, az, hero, 4*\text{max\_action\_time} + \text{max\_elevator\_wait}). (The notation “4*\text{max\_action\_time}” here and similar notations below should be taken as syntactic sugar for “\text{max\_action\_time} + \text{max\_action\_time} + \text{max\_action\_time} + \text{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 \text{time}(s5) + \text{max\_action\_time}, so by lemma B.27 reserved\_block(time(s6), az, hero, 3*\text{max\_action\_time} + \text{max\_elevator\_wait}).

We now have a hierarchical case analysis.

\textbf{Case 1:} Suppose that holds(s6, has(az, b1)) and \neg holds(s6, \text{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*\text{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, \text{elevator\_at}(az)). We have reserved\_block(time(s9), az, hero, 2*\text{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 $s_{11}$ be the first situation such that $s_1 \leq s_{11} \leq s_{10}$, holds($s_{11}$, elevator_at($az$)), choice($az$, $s_{11}$) and reserved_block(time($s_{11}$), $az$, hero, max_action_time).

There are now two cases to consider:

**Case 1.1:** Suppose that holds($s_{11}$, has($az$, $b_1$)). Then $el_2.q_2$($az$, $s_{11}$, $s_0$), so the result follows from lemma B.57.

**Case 1.2:** Suppose that $\neg$ holds($s_{11}$, has($az$, $b_1$)). Then by lemma B.43, holds($s_{11}$, loaded_since($b_1$, $az$, time($s_1$))). Let $s_{12}$ be the first situation such that $s_1 < s_{12} \leq s_{11}$, holds($s_{12}$, loaded_since($b_1$, $az$, time($s_1$))), choice($az$, $s_{12}$), and reserved(time($s_{12}$), $az$, hero). Then $el_2.q_3$($az$, $s_{12}$, $s_1$). The result then follows from lemma B.56.

**Case 2:** Suppose that holds($s_6$, has($az$, $b_1$)) and holds($s_6$, elevator_at($az$)). The proof continues in the same way as in case 1 from situation $s_9$ onward.

**Case 3:** Suppose that $\neg$ holds($s_6$, has($az$, $b_1$)). The proof continues in the same way as in case 1.2.

**Lemma B.59:**

$[AZ \neq \text{hero} \land \text{accepts_req}(el_2(AZ), AZ, hero, S_1) \land \text{holds}(S_1, \text{elevator_at}(AZ)) \land \text{holds}(S_1, \text{on_elevator}(b_1)) \land \text{elt}(S_1, I) \land \text{socposs_int}(I)] \Rightarrow \exists S_2, S_3, Z \ S_1 < S_2 < S_3 \land \text{elt}(S_3, I) \land \text{time}(S_3) \leq \text{time}(S_1) + \text{delay_time} + \text{min_reserve_block} \land \text{occurs(inform(AZ, robots, loaded_since(b_1, time(S_0))), S_2, S_3)}$.

**Proof:** Let $az, s_{11}, i_1, s_5, s_6$ be the same as in the proof of B.58. By XC.11, holds($s_6$, loaded_since($b_1$, $az$, time($s_1$))). The proof then continues as in Case 1.2 of lemma B.52.

**Validation of Plan el1**

**Lemma B.60:**

$\forall S_0, S \ S_0 < S \Rightarrow
[[\forall S_0, A \ S_0, A \iff \Phi(S_0, S_0, A) \vee \forall S_0, A \ S_0, A \iff \neg \Phi(S_0, S_0, A)]]$

where $\Phi$ is any of the relations “el1.q1”, “el1.q2”, “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:**

$el_1.q_1(S_1, S_0) \Rightarrow
[\text{know_next_step}(E, el_1, hero, S_1, S_0) \iff \text{instance}(E, \text{broadcast_req(hero, robots, r2)}, S_1)] \land
[\text{exec_cont}(E, el_1, hero, hero, S_1, S_0) \iff \text{instance}(E, \text{broadcast_req(hero, robots, r2)}, S_1)]$

**Proof:** By XD.2, MD.2, MD.3, $S_1$ is a choice point for hero. By X.2, the only next steps of el1 in $S_1$ 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 $S_1$. 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 $S_1$.

**Lemma B.62:**

$el_1.q_2(S_1, S_0) \Rightarrow
[\text{know_next_step}(E, el_1, hero, S_0, S_0) \iff E=\text{do(hero, call)}] \land
[\text{exec_cont}(E, el_1, hero, hero, S_1, S_0) \iff E=\text{do(hero, call)}]$.

**Proof:** Analogous to lemma B.61.

**Lemma B.63:**
el1 \(q_3(S_1, S_0) \Rightarrow \)
\[\text{know\_next\_step}(E, el1, hero, S_0, S_0) \iff E = \text{do}(hero, \text{unload}(b_1)) \land \text{exec\_cont}(E, el1, hero, hero, S_1, S_0) \iff E = \text{do}(hero, \text{unload}(b_1))].

**Proof:** Analogous to lemma B.61.

**Lemma B.64:**
\[\text{working\_on}(el1, hero, hero, S_0, S_1) \land \text{elt}(S_1, I) \land \text{soc\_poss\_int}(I) \land \text{el1\_q1}(S_1, S_0) \Rightarrow \text{leads\_towards1}(\text{broadcast\_req}(hero, robots, r_2), S_1, I).\]

**Proof:** From B.53, B.61.

**Lemma B.65:**
\[\text{working\_on}(el1, hero, hero, S_0, S_1) \land \text{elt}(S_1, I) \land \text{soc\_poss\_int}(I) \land \text{el1\_q2}(S_1, S_0) \Rightarrow \text{leads\_towards1}(\text{do}(hero, \text{call}), S_1, I).\]

**Proof:** From B.53, B.62.

**Lemma B.66:**
\[\text{working\_on}(el1, hero, hero, S_0, S_1) \land \text{elt}(S_1, I) \land \text{soc\_poss\_int}(I) \land \text{el1\_q3}(S_1, S_0) \Rightarrow \text{leads\_towards1}(\text{do}(hero, \text{unload}(b_1)), S_1, I).\]

**Proof:** From B.53, B.63.

**Lemma B.67:**
begin\_plan(el1, hero, hero, S_0, S_1) \land \text{terminates}(el1, hero, hero, S_0, S_1) \Rightarrow \text{know\_succeeds}(el1, hero, S_0, S_1).

(Plan el1 can only terminates with success.)

**Proof:** Suppose that begin(el1, hero, hero, S_0, S_1) and ¬know\_succeeds(el1, hero, hero, S_0, S_1). We wish to show that el1 does not terminate in S_1. There are two cases to consider:

**Case 1:** S_1 = S_0 or el1\_q2(S_1, S_0) or el1\_q3(S_1, S_0). By lemmas B.61, B.62, B.63 there is an executable continuation for el1 in S_1; hence by QD.2, QD.3, QD.5, el1 does not terminate in S_1.

**Case 2:** S_1 ≠ S_0 and ¬el1\_q2(S_1, S_0) and ¬el1\_q3(S_1, S_0). If S_1 is not a choice point for the hero, then el1 does not terminate in S_1 (QD.3, QD.4, QD.5), so assume that S_1 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 S_1 ≠ S_0, ¬el1\_q2(S_1, S_0), and ¬el1\_q3(S_1, S_0). so he knows that any action of his 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:**
\[\text{el1\_q1}(AZ, S_2, S_1) \Rightarrow \exists E \text{\ instance}(E, \text{broadcast\_req}(AZ, robots, r_2), S_2) \land \text{feasible}(E, S_2).\]

**Proof:** By axiom E.16, it is feasible for AZ to communicate to robots. By C.5, broadcast(AZ,robots,r2) is feasible in S_2. By C.6, know\_how(AZ,broadcast(AZ,robots,r2),S_2). The result follows from MD.1 and KHD.1.

**Lemma B.69:**
\[\text{working\_on}(el1, hero, hero, S_0, S_0) \land \text{elt}(S_0, I_0) \land \text{soc\_poss\_int}(I_0) \land \forall_{AZ, r_2} AZ \neq hero \Rightarrow \neg\text{working\_on}(P_2, AZ, hero, S_0, S_0)) \Rightarrow \exists_{SZ} SZ \geq S_0 \land \text{elt}(SZ, I) \land \text{completes}(el1, hero, hero, S_0, SZ).\]

**Proof:**
Assume that $s_0$ and $i_0$ satisfy the left hand of the implication. Let $s_1$ be the first situation after $s_0$ in $i_0$ such that reserved(time($s_1$), hero, hero) and choice(hero,$s_1$). By Q.2, QD.1, X.7, such an $s_1$ will occur in $i_0$ within time at most delay_time + max_action_time of $s_0$. By XD.3, $e_{l_1,q_1}(s_1,s_0)$. By lemma B.68, there is a situation $s_2$ in $i_0$ such that occurs(broadcast_req(hero, robots, r2), s1, s2). By S.6, the event request(hero, A2 assignment(r2, A2)) occurs from $s_1$ to $s_2$ for every agent $A_2 \neq hero$.

By lemma B.67 and B.36, either $el_1$ has completed before $s_2$ or hero is still working on $el_1$ in $s_2$. If $el_1$ has completed, then that completes the proof, so assume that $el_1$ has not completed. By X.2 and lemma B.33, hero does not issue any broadcasts other than $r_2$ between $s_0$ and $s_2$. By S.7, hero does not make any requests of $A_2$ between $s_0$ and $s_2$. By Q.6, $A_2$ has not accepted any other requests of hero between $s_0$ and $s_2$. By Q.5, $A_2$ is not working on any plans of hero at $s_2$. By Q.6, $A_2$ accepts the request assignment(r2, A2).

By lemma B.67 and B.36, either $el_1$ has completed before $s_2$ or hero is still working on $el_1$ in $s_2$. If $el_1$ has completed, then that completes the proof, so assume that $el_1$ has not completed. By X.2 and lemma B.33, hero does not issue any broadcasts other than $r_2$ between $s_0$ and $s_2$. By S.7, hero does not make any requests of $A_2$ between $s_0$ and $s_2$. By Q.6, $A_2$ has not accepted any other requests of hero between $s_0$ and $s_2$. By Q.5, $A_2$ is not working on any plans of hero at $s_2$. By Q.6, $A_2$ accepts the request assignment(r2, A2).

By lemma B.67 and B.36, either $el_1$ has completed before $s_2$ or hero is still working on $el_1$ in $s_2$. If $el_1$ has completed, then that completes the proof, so assume that $el_1$ has not completed. By X.2 and lemma B.33, hero does not issue any broadcasts other than $r_2$ between $s_0$ and $s_2$. By S.7, hero does not make any requests of $A_2$ between $s_0$ and $s_2$. By Q.6, $A_2$ has not accepted any other requests of hero between $s_0$ and $s_2$. By Q.5, $A_2$ is not working on any plans of hero at $s_2$. By Q.6, $A_2$ accepts the request assignment(r2, A2).

By E.12, E.13 there is an agent az such that, in $s_2$, either az has $b_1$ or [the elevator is at az and $b_1$ is loaded on the elevator]. By lemmas B.58, B.59 there exist situations $s_3, s_4$ in $i_0$ such that occurs(inform(az, robots, loaded since(b1, az, time(s0))), s3, s4), and $s_4$ in $i_0$. By C.2, CK.1, the hero knows in $s_4$ that $a_2$ has informed him of this fact; that is, in every situation $S_A B$ accessible from $s_4$, it is the case that there exists an $S_A B$ accessible from $s_4$ and $S_A B < S_A B$ 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 $s_5$ be the first situation after $s_4$ in $i_0$ such that reserved block(time($s_5$), hero, hero, $3*max_{action}$ time + $max_{elevator}$ wait). By Q.2, X.7, time($s_5$) $\leq$ time($s_4$) + delay_time. Suppose that $k_{acc(hero,s_5,S_5)}$. By lemma B.50, b1 is on the elevator in $S_5 B$. Thus by XD.1 holds($s_5$, know Loaded(hero, b1)); hence, in $s_5$ it is the case that $S_5 B$.

There are now two cases to consider:

**Case 1:** Suppose that $el_1 q_3(S,s_0)$ does not hold for any $S$ between $s_0$ and $s_6$. Then el1_q12(s6, s0) (XD.4, XD.5). By lemma B.62 there exists $s_7$ in $i_0$ such that occurs(do(hero, call), s6, s7). Using E.4, FD.6, let $s_8$ be the first situation in $i_0$ such that time($s_8$) $\leq$ time($s_7$) + $max_{elevator}$ wait $\leq$ time($s_6$) + $max_{action}$ time + $max_{elevator}$ wait and holds(s8, elevator at(hero)). Let $s_9$ be the first choice point for hero in $i_0$ after $s_8$; thus time($s_9$) $\leq$ time($s_8$) + $max_{action}$ time. By E.7, E.1, the elevator is still at the hero in $s_9$; by B.50 package b1 is still on the elevator in $s_9$; and time($s_9$) is still reserved by the hero for himself. Let $s_10$ be the first choice point in $i_0$ after $s_0$ such that in $s_10$ the elevator is at the hero, the package is on the elevator and the time is reserved by the hero for himself. Then $el_1 q_3(s_10, s_0)$. By Q.2, time($s_10$) $\leq$ time($s_9$) + delay_time. By lemma B.66, occurs(do(hero, unload(b1)), s10, s11) for some $s_11$ in $i_0$. Thus $s_11$ satisfies the right hand side of the implication.

**Case 2:** Suppose that $el_1 q_3(S,s_0)$ holds for some $S$ between $s_0$ and $s_6$. Then the proof continues as in Case 1, from $s_10$ on.

**Lemma B.70:** $k_{acc(hero,s_0,S_0A)} \Rightarrow executable(el_1, hero, S_0A)$

**Proof:** Assume that $k_{acc(hero,s_0,S_0a)}$, occurs(do(hero, commit(hero, el1)), s0a, s1a), elt(s1a, i0), and soc_pos int(i0). By X.13 $\exists_{P,A,C,SX}$ working on($P,A,C,hero,SX,s_0a$); that is, in $s_0a$ no one including hero is working on any plans of hero’s. Since no other commit or broadcast actions occur between $s_0a$ and $s_1a$ (axioms A.1, A.2), no other requests occur (S.7) or are accepted (Q.6); hence, in $s_1a$ 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 $s_0a$ (Q.11).
Theorem B.71: $\text{know\_achievable}(\text{has(hero,b1)}, \text{el1}, \text{hero}, s0)$.  

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