How Does a Box Work? : Appendix. Formal proof of correctness of plan1

Ernest Davis*
Dept. of Computer Science
New York University
davise@cs.nyu.edu

September 5, 2008

Note: Unlike the main article, I have not put constant symbols into typewriter font in this proof. There is only so much time I want to spend making fiddly typographical edits in a document that probably no one will ever read. I have not tidied up the numbering on lemmas/definitions for the same reason.

One necessary constraint in the problem specification was accidentally deleted from the current draft of the paper

P1.37 holds(s1,rccEC$^{\#}$(manipSpace1,oTable2)).

1 Plan Execution

Lemma 1.1:
historyProperPrefix$(H1, H2) \Leftrightarrow$
$\exists_{HM}$ historyProperPrefix$(H1, HM) \wedge$ historyProperPrefix$(HM, H2)$.

Proof: From definitions TD.15, TD.14, TD.13, axiom T.4, plus transitivity of ordering and the density of time points, inherited from real numbers. ∎

In general below, I will omit the aspects of proofs that depend purely on unrolling definitions TD.1 – TD.23 or that depend on applying the properties of the real numbers to time points.

Lemma 1.2:
$\forall_{P,H,H1}$ beginsxE$(P, H) \wedge$ historyProperPrefix$(H1, H) \Rightarrow$ begins$(P, H1)$

Proof: Suppose that beginsxE(P, H) and historyProperPrefix$(H1, H)$. Using PLD.3, since start$(H1)$=start(H) we have beginnable(P,start$(H1)$). For any $H2$, if historyProperPrefix$(H2, H1)$ then by lemma 1.1 historyProperPrefix$(H2, H)$ and holds(start(H),kinematicState), so by PLD.3 baseExec$(P, H2)$. Hence by PLD.3, begins$(P, H1)$. ∎

Lemma 1.3:
$\forall_{P,H}$ beginnable(P,start(H)) $\wedge$ [$\forall_{H1}$ historyProperPrefix$(H1, H) \Rightarrow$ beginsxE$(P, H1)$] $\Rightarrow$ beginsxE(P, H)

*This research was supported in part by NSF grants IIS-0097537, and IIS-0534809.

Proof: Suppose that $\forall_{H1}$ historyProperPrefix$(H1, H) \Rightarrow$ beginsxE$(P, H1)$. Let $H2$ be any history such that historyProperPrefix$(H2, H)$. By lemma 1.1, there exists a history $H3$ such that historyProperPrefix$(H2, H3)$ and historyProperPrefix$(H3, H)$. Therefore, by assumption beginsxE$(P, H3)$. By PLD.3, since $H2$ is a proper prefix of $H3$, baseExec$(P, H2)$. Therefore, applying PLD.3 from right to left, beginsxE(P, H). ∎

Lemma 1.4:
$\forall_{H,P}$ begins$(P, H) \Rightarrow \exists_J$ historyPrefix$(H, J) \land$ attempts(P, J).

Proof: By PLD.3—PLD.8, attempt(P, J) holds if J is a maximal history such that begins(P, H) holds overall all prefixes or proper prefixes H of J. Axiom HC.3 guarantees the existence of such a maximal history.

To spell this out in greater detail: Axiom schema HC.3 applied to the formula $\Phi(\cdot)$=begins$(P, \cdot)$ gives the statement

$\forall_H$ begins$(P, H) \Rightarrow$
$\exists_J$ historyPrefix$(H, J) \land$
$\quad\forall_{H1}$ [historyProperPrefix$(H1, J) \Rightarrow$ begins$(P, H1)] \land$
$\qquad$[historyProperPrefix$(J, H1) \Rightarrow$
$\qquad\exists_{H2}$ historyPrefix$(J, H2) \land$ historyPrefix$(H2, H1) \land \neg$begins$(P, H2)]]$.

Assume that begins(P, H) and let J satisfy the right-hand side of the above implication. By PLD.4, PLD.5, beginnable(P,start(H)). By lemmas 1.2, 1.3 the property of J
$\quad\forall_{H1}$ [historyProperPrefix$(H1, J) \Rightarrow$ begins$(P, H1)$]
is in fact just equivalent to beginsxE(P, J).

The property of J,
$\quad\forall_{H1}$ [historyProperPrefix$(J, H1) \Rightarrow$
$\qquad\exists_{H2}$ historyPrefix$(J, H2) \land$ historyPrefix$(H2, H1) \land \neg$begins$(P, H2)]]$
is the negation of
$\quad\exists_{H1}$ [historyProperPrefix$(J, H1) \land$
$\qquad\forall_{H2}$ historyPrefix$(J, H2) \land$ historyPrefix$(H2, H1) \Rightarrow$ begins$(P, H2)]]$

Since P also begins over all proper prefixes of J, by lemma 1.2, this is equivalent to
$\quad\exists_{H1}$ historyProperPrefix$(J, H1) \land$ beginsxE$(P, H1)$.

Now there are two possibilities: either continuableEnd$(P, H1)$ or not. If continuableEnd$(P, H1)$ then by PLD.6 there exists $H2$ such that sameUntilEnd$(H1, H2)$ and begins$(P, H2)$. ∎

Lemma 1.5: $\forall_{S,P}$ holds(S,kinematicState) $\Rightarrow \exists_J$ start(J)=$S \land$ attempts(P, J).

Proof: Using T.3 choose $H1$ such that singleHist$(H1, S)$. If $\neg$beginnable(P, S) then the result is immediate from PLD.5 with $J = H1$. Otherwise, it follows from PLD.3 that begins$(P, H1)$ (the quantified condition holds vacuously), so the result follows from lemma 1.4. ∎

Lemma 1.6:
attempts$(P, J1) \land$ historyProperPrefix$(J1, J2) \Rightarrow \neg$attempts$(P, J2)$.

Proof: Immediate from PLD.5, PLD.4, PLD.3. ∎

Lemma 1.7:
completes$(P, J1) \land$ historyProperPrefix$(J1, J2) \Rightarrow \neg$completes$(P, J2)$.

Proof: Immediate from PLD.6, Lemma 1.6. ∎

Lemma 1.8:

reactComplete(P, H) $\wedge$ historyProperPrefix($H, H1$) $\Rightarrow$ reactComplete($P, H1$).

Proof: Immediate from PLD.1. A time TC and history HC that satisfies the right side of PLD.1 for H also satisfies it for $H1$. ▮

Lemma 1.9:
baseExec(P, H) $\wedge$ historyPrefix($H1, H$) $\Rightarrow$ ¬completes($P, H1$).

Proof: By PLD.1, ¬reactComplete(P, H). By lemma m1, ¬reactComplete($P, H1$). The result follows from PLD.6. ▮

Lemma 1.10: attempts(P, H) $\wedge$ [holds(start(H),kinematicState) $\vee$ ¬singleHist(H,start(H))] $\Rightarrow$ dynamic(H).

Proof: If singleHist(H,start(H)) then start(H) is kinematic, so by DYN.3 dynamic(H). Otherwise, the result is immediate from PLD.7, PLD.4, PLD.3. ▮

Lemma 1.11
reactComplete(P, H) $\Rightarrow$
$\exists_{H1}$ historyPrefix($H1, H$) $\wedge$ reactComplete($P, H1$) $\wedge$
$\forall_{H2}$ historyProperPrefix($H2, H1$) $\Rightarrow$ ¬reactComplete($P, H2$).

Proof: Let $\Phi(T)$ be the following property:

$$\text{startTime}(H) \leq T \wedge \exists_{HA}\ \text{historySlice}(H,\text{startTime}(H),T,HA) \wedge \text{reactComplete}(P, HA).$$

By lemma 1.8, if $\Phi(T1)$ and $T1 < T2$ then $\Phi(T2)$. Since Φ(endTime(H)), by the Dedekind property there is a minimal TX dividing the times where Φ holds from those where it does not. By PLD.1, Φ holds on TX, and the conditions of the lemma hold if $H1$ is the prefix of H ending at TX. ▮

Lemma 1.12:
reactComplete(P, H) $\Rightarrow$ endTime(H) $-$ startTime(H) $\geq$ reactionTime.

Proof: Immediate from PLD.1. ▮

Lemma 1.13:
completes(P, H) $\Rightarrow$ beginnable(P,start(H)).

Proof: By PLD.6 attempts(P, H) and reactComplete(P, H). By PLD.5, if attempts(P, H) and ¬beginnable(P,start(H)) then H is instantaneous, but by Lemma 1.12, the duration of H must be at least reactionTime. Hence beginnable(P,start(H)). ▮

Lemma 1.14:
baseExec(P, H) $\Rightarrow$ $\neg\exists_{H1}$ historyPrefix($H1, H$) $\wedge$ completes($P, H1$). ▮

Proof: PLD.1, PLD.2, PLD.6, lemma 1.8. ▮

1.1 Control Structures

Lemma 1.15
baseExec($P1, H$) $\Rightarrow$ baseExec(sequence($P1, P2$),H)

Proof: Assume baseExec($P1, H$). By PLD.2, CTL.2, lemma 1.14, worksOn(sequence($P1, P2$),H). Let $H1$ be a prefix of H that ends earlier than endTime(H)$-$reaction Time. By PLD.1, PLD.2, ¬completion($P1, H1$). Let HA be any prefix of H. By lemma 1.9, completes($P1, HA$) does not hold; hence by CTL.3, completion(sequence($P1, P2$),HA) does not hold; hence by PLD.1 ¬reactComplete(sequence($P1, P2$),H). By PLD.2, beginnable(sequence($P1, P2$),start(H)) and holds(start(H),kinematicState

Thus, we have met all the conditions for
baseExec(sequence($P1, P2$),H) on the right side of PLD.2. ∎

Lemma 1.16
completes($P1, H1$) $\wedge$ baseExec($P2, H2$) $\wedge$ hsplice($H1, H2, H$) $\Rightarrow$
baseExec(sequence($P1, P2$),H).

Proof: By lemma 1.10, dynamic($H1$) and by PLD.2 dynamic($H2$) so by DYN.7 dynamic(H). By PLD.2, CTL.2 worksOn(sequence($P1, P2$),H). By PLD.1, PLD.2, completion($P2, HA$) does not hold for any prefix HA of $H2$ that ends earlier than endTime(H)−reactionTime. By lemma 1.7, PLD.3 completion(sequence($P1, P2$),HB) does not hold for any prefix HB of H that ends ealier than endTime(H)− reactionTime. By PLD.1 ¬reactComplete(sequence($P1, P2$),H). By lemma 1.12 beginnable($P1$,start(H)); hence by CTL.1 beginnable(sequence($P1, P2$),start(H)). Thus, we have met all the conditions for baseExec(sequence($P1, P2$),H) on the right side of PLD.2. ∎

Lemma 1.17:
begins($P1, H$) $\Rightarrow$ begins(sequence($P1, P2$),H).

Proof: Immediate from CTL.1, PLD.3, lemma 1.15. ∎

Lemma 1.18:
completes($P1, H1$) $\wedge$ begins($P2, H2$) $\wedge$ hsplice($H1, H2, H$) $\Rightarrow$
begins(sequence($P1, P2$),H).

Proof: Immediate from CTL.1, PLD.3, lemma 1.16. ∎

Lemma 1.19: FIX
begins(sequence($P1, P2$),J) $\Rightarrow$
[begins($P1, J$) $\wedge$ ¬completes($P1, J$)] $\vee$
[completes($P1, J$) $\wedge$ ¬beginnable($P2$,end(J))] $\vee$
[$\exists_{H1,J2}$ completes($P1, H1$) $\wedge$ begins($P2, J2$) $\wedge$ hsplace($H1, J2, J$)].

Proof: There are three cases.

Case 1: There is no prefix $H1$ of J such that completes($P1, H1$). Let HA be any proper prefix of J. By PLD.3, PLD.2 dynamic(HA) and worksOn(sequence($P1, P2$),HA). By CTL.2 worksOn($P1, HA$).

Suppose that reactComplete($P1, HA$). Using lemma 1.11, let HC be the minimal prefix of HA for which reactComplete($P1, HA$). Then by PLD.9 completes($P1, HC$) contrary to assumption. Thus ¬reactComplete($P1, HC$). By PLD.3 incompleteExec($P1, HA$). By CTL.1, beginnable(P,start(H)). Hence by CTL.3 begins($P1, J$).

Case 2: There is a prefix $H1$ of J such that completes($P1, H1$). but ¬beginnable($P2$,end($H1$)). By PLD.2 ¬baseExec(sequence($P1, P2$),$H1$). Thus by PLD.3 begins(sequence($P1, P2$),$H2$) does not hold for any proper extension $H2$ of $H1$; hence J is not a proper extension of $H1$; hence $J = H1$.

Case 3: There is a prefix $H1$ of J such that completes($P1, H1$). and beginnable($P2$,end($H1$)). Let $J2$ be the history such that hsplice($H1, J2, H$). If $J2$ consists of a single situation, then begins($P2, H2$) is immediate from CTL.3. Otherwise, let $H3$ be any history such that $H1$ is a prefix of $H3$ and $H3$ is a proper prefix of J. By PLD.3, PLD.2, worksOn(sequence($P1, P2$),$H3$), so by CTL.2 worksOn($P2, H3$). By assumption beginnable($P2, H3$). By PLD.1, CTL.3 ¬reactComplete($P2, H3$). By DYN.5 dynamic($H3$). Hence by PLD.2 baseExec($P2, H3$). Hence by PLD.3 begins($P2, J2$). ∎

Lemma 1.20:
begins(sequence($P1, P2$),J) $\Leftrightarrow$
[begins($P1, J$) $\wedge$ ¬completes($P1, J$)] $\vee$
[completes($P1, J$) $\wedge$ ¬beginnable($P2$,end(J))] $\vee$
$\exists_{H1,J2}$ completes($P1, H1$) $\wedge$ begins($P2, J2$) $\wedge$ hsplice($H1, J2, J$)].

Proof: Putting together 1.17, 1.18, 1.19. ▮

Lemma 1.21:
attempts(sequence($P1, P2$),J) $\Leftrightarrow$
[attempts($P1, J$) $\wedge$ ¬completes($P1, J$)] $\vee$
[completes($P1, J$) $\wedge$ ¬beginnable($P2$,end(J))] $\vee$
$\exists_{H1,J2}$ completes($P1, H1$) $\wedge$ begins($P2, J2$) $\wedge$ hsplice($H1, J2, J$)]

Proof: Immediate from lemma 1.20, PLD.5. ▮

Lemma 1.22:
completes(sequence($P1, P2$),H) $\Leftrightarrow$
$\exists_{H1,H2}$ completes($P1, H1$) $\wedge$ completes($P2, H2$) $\wedge$ hsplice($H1, H2, H$)]

Proof: Immediate from lemma 1.21, PLD.6, CTL.3, PLD.1.

Proof: Straightforward definition chasing through from CTL.6 through CTL.10, PLD.1 through PLD.3

Definition 1.23:
noopStart(H: history) $\equiv$
dynamic(H) $\wedge$ throughoutxSE(H,freeGrasp) $\wedge$ endTime(H) $\leq$ startTime(H) + reactionTime.

Definition 1.24:
noop(H: history) $\equiv$
dynamic(H) $\wedge$ throughoutxSE(H,freeGrasp)) $\wedge$ endTime(H) = startTime(H) + reactionTime.

Lemma 1.25
begins(if1(Q, P),H) $\Leftrightarrow$
[holds(Q,start(H)) $\wedge$ begins(P, H)] $\vee$
[¬holds(Q,start(H)) $\wedge$ noopStart(H)].

Proof: CTL.7, PLD.1—PLD.4, definition 1.23.

Lemma 1.26:
attempts(if1(Q, P),H) $\Leftrightarrow$
[holds(Q,start(H)) $\wedge$ attempts(P, H)] $\vee$
[¬holds(Q,start(H)) $\wedge$ noop(H).]

Proof: Lemma 1.25, PLD.4, PLD.5, definition 1.24. ▮

Lemma 1.27:
completes(if1(Q, P),H) $\Leftrightarrow$
[holds(Q,start(H)) $\wedge$ completes(P, H)] $\vee$
[¬holds(Q,start(H)) $\wedge$ noop(H)].

Proof: Lemma 1.26, PLD.6. ▮

Lemma 1.28:
attempts(while(Q, P),J) $\Leftrightarrow$
[¬holds(start(J),Q) $\wedge$ noop(J)] $\vee$
[holds(start(J),Q) $\wedge$ attempts(P, J) $\wedge$ ¬completes(P, Q)] $\vee$
[holds(start(J),Q) $\wedge$ $\exists_{H1,J2}$ completes($P, H1$) $\wedge$ attempts(while(Q, P),$J2$) $\wedge$ hsplice($H1, J2, J$)].

Proof: Axiom CTL.12 together with Lemmas 1.26 and 1.21. ▮

Lemma 1.29:
completes(while(Q, P),J) $\Leftrightarrow$
[¬holds(start(J),Q) $\wedge$ noop(J)] $\vee$

[holds(start(J),Q) $\wedge$ $\exists_{H1,J2}$ completes($P, H1$) $\wedge$ completes(while(Q, P),$J2$) $\wedge$ hsplice($H1, J2, J$)].

Proof: Lemmas 1.27 and CS.8. ∎

Lemma 1.30: Let $\Phi(S{:}\text{state},X)$ be an open formula with free variable S and optionally other variables X. The following holds:

$$
\begin{array}{l}
\forall_{P,P1:\text{plan},H:\text{history},Q:\text{fluent[Bool]},X} \\
\quad [P{=}\text{while}(Q,P1) \wedge \text{attempts}(P,H) \wedge \Phi(\text{start}(H),X) \wedge \\
\quad\; [\forall_{H1:\text{history}}\ [\Phi(\text{start}(H1),X) \wedge \text{holds}(\text{start}(H1),Q) \wedge \text{attempts}(P1,H1) \Rightarrow \\
\qquad\qquad\qquad \text{completes}(P1,H1) \wedge \Phi(\text{end}(H1),X)] \wedge \\
\qquad\qquad\quad [\Phi(\text{start}(H1),X) \wedge \neg\text{holds}(\text{start}(H1),Q) \wedge \text{noop}(H1) \Rightarrow \Phi(\text{end}(H1),X)] \\
\quad\;]] \Rightarrow \\
\quad \text{completes}(P,H) \wedge \Phi(\text{end}(H),X).
\end{array}
$$

Proof: By induction over $\lfloor(\text{endTime}(H){-}\text{startTime}(H)\ /\ \text{reactionTime}\rfloor$ (an upper bound on the number of completed iterations).

Assume that the left-hand side of the implication above holds; that is:

a. P=while($Q, P1$) $\wedge$ attempts(P, H) $\wedge$ Φ(start(H),X).

b. $\forall_{H1}$ Φ(start($H1$),X) $\wedge$ holds(start($H1$),Q) $\wedge$ attempts($P1, H1$) $\Rightarrow$
[completes($P1, H1$) $\wedge$ Φ(end($H1$),X)]

c. $\forall_{H1}$ Φ(start($H1$),X) $\wedge$ $\neg$holds(start($H1$),Q) $\wedge$ noop($H1$) $\Rightarrow$ Φ(end($H1$),X)]

Base case: If $\lfloor(\text{endTime}(H){-}\text{startTime}(H)\ /\ \text{reactionTime}\rfloor = 0$, and attempts($P, H$), then the first and third disjunctions of lemma 1.28 (the condition fails and a no-op is executed, or the condition succeeds and the first iteration of P completes) cannot hold, since either a no-op or a complete execution of a plan takes at least reactionTime (lemma 1.12). Thus the second disjunct must hold; that is holds(start(J),Q) $\wedge$ attempts($P1, J$) $\wedge$ $\neg$completes($P1, Q$). But this contradicts condition (b) above, so the overall implication is true vacuously.

Inductive case: Assume that the lemma holds for all histories $H1$ where
$\lfloor(\text{endTime}(H1){-}\text{startTime}(H1))\ /\ \text{reactionTime}\rfloor{=}K$ for some value of K. Let H be a history such that
$\lfloor(\text{endTime}(H1){-}\text{startTime}(H1))\ /\ \text{reactionTime}\rfloor{=}K+1$ Assume that the left-hand side of the implication holds. Since attempts(while($Q, P1$),H), by 1.28 there are three cases:

Case 1: $\neg$holds(start(H),Q) and noop(H).
By condition (c) and lemma 1.29 completes(P, H).

Case 2: holds(start(H),Q), attempts(P, H) and $\neg$completes(P, H).
This is excluded by condition (b).

Case 3: holds(start(J),Q) $\wedge$
$\exists_{H1,J2}$ completes($P, H1$) $\wedge$ attempts(while(Q, P),$J2$). $\wedge$ hsplice($H1, J2, J$).
By condition (c), Φ(end($H1$),X). By lemma 1.12, $H1$ has duration at least reactionTime; hence (endTime($J2$)$-$startTime($J2$)) $\leq K$, so the inductive hypothesis applies to $J2$. Clearly $J2$ satisfies all of conditions (a), (b), and (c); hence by the induction hypothesis completes($P, J2$) and Φ(end($J2$),X). Since end($J2$)=end(H), we have Φ(end(H),X). By lemma 1.29 we have completes(P, H).
∎

Lemma 1.31:

[sort(Q)=fluent[objectSet] $\wedge$ P=while ($Q \neq^{\#} \emptyset, P1$), J) $\wedge$ attempts(P, J) $\wedge$
[$\forall_{J1}$ historySlice($J1, J$) $\wedge$ attempts($P1, J1$) $\Rightarrow$
history($J1$) $\wedge$ count(value(end($J1$),Q)) < count(value(start($J1$),Q))]] $\Rightarrow$
history(J).

Proof: By a simple induction on count(value(start(J),Q)). ▮

(Note: To aid readability, we are abusing notation here and below in using count($\cdot$) as a function rather than as a two-place predicate.)

Definition 1.32: throughoutxS(H, Q) $\Leftrightarrow$
$\forall_{T,S}$ stateAt(H, T, S) $\wedge$ startTime(H)< T $\Rightarrow$ holds(S, Q).

Lemma 1.33:
attempts(waitUntil(Q),J) $\Rightarrow$
throughoutxS(J,freeGrasp) $\wedge$
[[unbounded(J) $\wedge$ throughout($J, \neg^{\#} Q$))] $\vee$
[bounded(J) $\wedge$ completes(waitUntil(Q),J)]].

Proof: Let P=waitUntil(Q). By AC.4 P is always beginnable. Hence, if attempts(P, J) by PLD.7 either [begins(P, J) and $\neg$continuable(P, J)] or [beginsxE(P, J) and $\neg$continuableEnd(P, J)]. In either case, by PLD.4, PLD.3, prefixes $H1$ of J, baseExect($P, H1$), so by PLD.2 reactComplete($P, H1$) is false and worksOn($P, H1$) is true. Hence by AC.5 freeGrasp is true at all times before the end of J. By AC.6 and PLD.1 if J is unbounded then Q is always false; if J is bounded, then Q is false at all times before endTime(J)$-$reactionTime.

Suppose that J is bounded and that the above disjunct beginsxE(P, J) and $\neg$continuableEnd(P, J) is true. Let $H1$ be a history satisfying DYN.10; that is, $H1$ is identical to J up to but not including end(J) and holds(end($H1$),freeGrasp). By AC.5, worksOn(P, J). By PLD.5 since $\neg$continuableEnd(P, J), it follows that $\neg$baseExec($P, H1$). By PLD.2, AC.6, it follows that reactComplete($P, H1$). Since $H1$ and J are identical at all times before endTime($H1$), it is immediate from PLD.1 that reactComplete(P, J). Therefore by PLD.8 completes(P, J).

The argument for the case where the disjunct begins(P, J) and $\neg$continuable(P, J) holds is almost identical. ▮

2 Loading loop

Definition 2.1:
Let loadedBelow(DH: distance) be the fluent whose value in S is the set of objects loaded in the box whose center of mass is below height DH. Formally,
$O \in$ value(S,loadedBelow(DH)) $\Leftrightarrow$
holds(S,$O \in^{\#}$loadedCargo $\wedge^{\#}$ height$^{\#}$($\uparrow$centerOfMass(O)) $\leq^{\#}$ DH)

(Note: Strictly, establishing the existence of such a fluent would require a comprehension axiom on fluents like axiom I.5 of [1]. However, nothing in this proof actually demands that these fluents exist as reified entities; we could just as well define the concept as a predicate loadedBelow(DH, S), and similarly the fluents defined below. The fluent notation is just to aid readability.)

Definition 2.2:
holds(S,midLoadingPosition) $\Leftrightarrow$
[sameStateOn(S,s1,{ oBox, oTable1 } $\cup$ value(S,unloadedCargo)) $\wedge$
holds(S,isolFluent(problem1)) $\wedge$

$\forall_D$ count(value(S, loadedBelow(bottom(rCuboid)+$D-$maxCargo))) $\geq$
min(count(value(S,loadedCargo)),
loadingCount(maxCargoDiam,lCube,wCube,D)))
].

Lemma 2.3:
[throughout(J,isolated(UM, UF)) $\wedge$ P=waitUntil(stable($UM \cup UF$)) $\wedge$ attempts(P, J) $\wedge$
$\forall_{O \in UF}$ fixed(UF)] $\Rightarrow$
completes(P, J).
(If a set of object UM is isolated from all but a set of fixed objects UF, and the agent waits long enough, everything will settle down to a stable position.)

Proof: Assume that the left-hand side holds. Suppose that J is unbounded. By lemma 1.33, freeGrasp and $\neg$stable($UM \cup UF$) hold throughout J. By DYD.1 throughout(J,isolated(UM, UF)). By H.3 there exists a suffix $J2$ of J throughout which stable($UM \cup UF$) holds, which is a contradiction.

Thus J is bounded, so by lemma 1.33 completes(P, J). ∎

Lemma 2.4:
$\forall_{O:\text{object},P1}$ $P1$ $\in$shape(O) $\Rightarrow$ distance($P1$,centerOfMass(O)) $\leq$ diameter(O).

Proof: Geometrically immediate from CM.2 ∎

Lemma 2.5:
holds(S,midLoadingPosition) $\Rightarrow$
$\forall_K$ $K \leq$ count(value(S,loadedCargo)) $\Rightarrow$
$\exists_U$ U $\subset$value(S,loadedCargo) $\wedge$ count(U) = K $\wedge$
$\forall_{O \in U}$ holds(S,top$^\#$($\uparrow O$) $<^\#$ bottom(rCuboid) $+^\#$ maxBottomHeight(K) + 2·maxCargoDiam).

Proof: Let D in definition 2.2 be chosen as maxBottomHeight(N) + 2·maxCargoHeight.
By definition 2.2 the number of loaded cargo objects whose center of mass is below
value(S,bottom(rCuboid)) + $D-$maxCargoDiam is at least
loadingCount(maxCargoDiam,lCube,wCube,D). By CM.2, PR.7, the top of any object is at most maxCargoDiam higher than its center of masss; hence the number of loaded cargo objects whose top is below bottom(rCuboid) + D is at least
loadingCount(maxCargoDiam,lCube,wCube,D); but this is at least N, by an arithmetic combination of P1.3.1, P1.3.2 and PR.23. ∎

Definition 2.6:
holds(S,freeCuboid(R)) $\equiv$
cuboid(R,maxCargoDiam,maxCargoDiam,2·maxCargoDiam) $\wedge$
R $\subset$rCuboid $\wedge$ holds(S,empty(R)) $\wedge$
bottom(R) = bottom(rCuboid) + value(S,maxBottomHeight$^\#$(count$^\#$(loadedCargo) + 1)))

Lemma 2.7:
holds(S,midLoadingPosition) $\Rightarrow$ $\exists_R$ holds(S,freeCuboid(R)).

Proof: Let N=count(value(S,loadedCargo)) and let $K = N + 1-$value(S,levelCount).
Let DB= bottom(rCuboid) + value(S,maxBottomHeight$^\#$(count$^\#$(loadedCargo)))
= bottom(rCuboid) + maxBottomHeight($N + 1$). By lemma 2.5, there are at least K loaded cargo objects whose top is below DB, so there are fewer than levelCount cargo objects with any part above DB.

Divide the slice of rCuboid between heights DB and DB + 2·maxCargoDiam into cuboids that are maxCargoDiam wide and deep and 2·maxCargoDiam high. There will 4·levelCount such cuboids. Clearly any single object can only intersect two cuboids in the x direction and two cuboids in the y-direction, hence can intersect a maximum of four cuboids. Since there are at most (levelCount−1) objects that intersect this slice, at most 4·(levelCount−1) of these cuboids are intersected by cargo objects. Thus there at least four cuboids that are not intersected by cargo objects. Since they are also not intersected by the box or by any unloaded object (Definition 2.2, PR.10, PR.20) or by any object outside o1 (PR.32, PR.18), they are empty and thus are free cuboids, by definition 2.6. ▮

Lemma 2.8:
holds(S,midLoadingPosition) $\wedge$ holds(S,freeCuboid(R)) $\wedge$
sameSituationExcept($S1, S, O$) $\wedge$ holds($S1$,$\uparrow O \subset^{\#} R$) $\Rightarrow$
holds($S1$,freeAbove(O)).

Proof: From the definition of freeAbove (P1.4) together with the fact that the free space above R is not intersected by any loaded cargo object, any unloaded cargo object or the box (Defn. 2.12, PR.10, PR.20) or any non-cargo object (PR.33, PR.18). ▮

Lemma 2.9:
$\forall_{RO,RB}$ cuboid(RB, L, W, D) $\wedge$ diameter(RO) $<$ min(L, W, D) $\Rightarrow$
$\exists_M$ translation(M) $\wedge$ imageMapping(M, RO) $\subset RB$.

Proof: Let M be the translation of RO that moves the bottommost point of RO to the bottom face of RB, the leftmost point of RO to the leftmost face of RB and the frontmost point of RO to the frontmost face of RB. ▮

Lemma 2.10:
holds(S,midLoadingPosition) $\wedge$ P $\in$manipSpace1 $\wedge$ oTable1Top+boxHeight $<$ height(P) $\Rightarrow$
$\neg\exists_{O:\text{object}}$ P $\in$value(S,place(O)).

Proof: Geometric from PR18, definition 2.2.

Lemma 2.11:
openBox(RB, RI, PST) $\wedge$
$[\forall_P\ P \in PST \Rightarrow$ height(P) = top(RI)] $\Rightarrow$
$\exists_{P1 \in \text{interior}(RI), P2 \in \text{interior}(RB)}$ pointAbove($P1, P2$).

Proof: Let PX be any interior point in RI, and let DB be a distance such that the ball of radius DX around PX is in RI. Let py(D)=$PX - D \cdot \hat{z}$ for $D \geq 0$. We have that py(0) = PX is inside RI, and, since RI is bounded, py(D) is outside RI for sufficiently large D. Hence there is a DX such that py(DX) is on the boundary of RI. Since PST is above PX, py(DX) is not in PST; hence (axiom SD.1) py(DX) is in boundary(RB). Since RB is regular, we can choose a point $P2$ in the interior of RB within DB of py(DX). Let $P1 = P2 + DX \cdot \hat{z}$. Since distance($P1, P2$) $< DB$, $P1$ is in the interior of $R1$. ▮

Corollary 2.11.A:
openBox(RB, RI, PST) $\wedge$
$[\forall_P\ P \in PST \Rightarrow$ height(P) = top(RI)] $\Rightarrow$
altogetherAbove(RI, RB).

Proof: Since RI is the closure of interior(RI) and RB is the closure of interior(RB), the result is immediate from lemma 2.11.

Lemma 2.12:
holds(S,midLoadingPosition) $\wedge$ O $\in$value(S,unloadedCargo) $\Rightarrow$
$\exists_{S1,M}$ sameSituationExcept($S1, S, O$) $\wedge$ holds($S1$,boxLoadingPos(O, QI)) $\wedge$ translation(M) $\wedge$
value($S1$,placement(O)) = imageMapping(M,value(S,placement(O)).

Proof: Use lemma 2.7 and lemma 2.9 to put O low down inside qInsideBox, then move O vertically downward until it comes into contact with some other object.

Formally: Let $R1$ be a region satisfying lemma 2.7. Let $M1$ be a translation satisfying Lemma 2.9, where $RB = R1$ and RO=value(S,place(O)).

For any $D \geq 0$ we will say that D is a *dropping* of $R1$ if the following holds:

$$\forall_{D1 \leq D, O1 \in \text{u1}} \text{ rccDC}(R1 - D1 \cdot \hat{z}, \text{ value}(S,\text{place}(O1))).$$

By definition $D = 0$ is a dropping of $R1$ and by lemma 2.11, for D sufficiently large, D is not a dropping of $R1$, since $R1 - D1 \cdot \hat{z}$ will overlap with value(S, ↑oBox)). Hence there is a maximum value of DM of D such that $D1$ is a dropping of R for all $D1 < DM$ and $D1$ is not a dropping of R for all $D1 > DM$. By continuity, $R1 - DM \cdot \hat{z}$ is externally connected to some object in u1. Let M=$M1 - DM \cdot \hat{z}$ and using DYN.1 let $S1$ be the state such that value(S,placement(O)) = M and sameStateExcept($S, S1, \{O\}$).

To establish the condition holds($S1$,boxLoadingPos(O, QI)), we must verify that
value ($S1$, height$^{\#}$(↑centerOfMass(O)) ≤ bottom(rCuboid) + maxBottomHeight(N) + maxCargo-Diam
where N=count(value($S1$,loadedCargo)). This follows immediately from the fact that the $N - 1$ objects in value(S,loadedCargo) are in the same position in $S1$ as in S, and hence have their center of mass below the specified height; that N=1+count(value(S,loadedCargo)); that bottom(O) is equal to or below bottom($R1$), which is at bottom(rCuboid)+maxBottomHeight(N); and that
value(S, height$^{\#}$(↑centerOfMass(O)) ≤ bottom(O)+maxCargoDiam.

The remaining conditions of holds(S,boxLoadingPos(O, QI)) and the remaining conditions on the right side of lemma 2.12 are immediate.

▮

Definition 2.13A:
holds(S,maximalConnectedGroup(U)) ≡
holds(S,connectedGroup(U)) ∧
$\forall_{O1}$ $O1 \notin U$ ⇒ ¬holds(S,connectedGroup($U \cup \{O1\}$).

Definition 2.13.B:
parallelMovable(O, S, HT, T) ≡
$\exists_{U1,HP}$ $O \in U1$ ∧ holds(S,maximalConnectedGroup($U1$)) ∧
start(HP)=S ∧ kinematic(HP) ∧
startTime(HP)=T ∧ sameMotion($HP, HT, \{O\}, 0$) ∧
[$\forall_{O1 \in U1}$ parallelMotion($O1, O, HP$)] ∧
[$\forall_{O1 \in \text{objectsOf}(HP) - U1}$ motionless($O1, HP$)].

Lemma 2.13:
sameStateOn(start(HT),start(H),{ O }) ∧ attempts(move(O, HT),H) ∧
endTime(H)−startTime(H) < endTime(HT)−startTime(HT) ⇒
¬ parallelMovable(O,end(H),HT,endTime(H)).

Proof: Let P=move(O, HT). Let D=startTime(H)−startTime(HT). By AC.3, ¬completion($P, H1$) for any prefix $H1$ of H, so by PLD.1 ¬reactComplete($P, H1$) for any prefix $H1$ of H. By AC.1 beginnable(P,start(H)). By PLD.7, either [beginsxE(P, H) and ¬continuableEnd(P, H)] or [begins(P, H) and ¬continuable(P, H)].

In either case (PLD.5) beginxE(P, H). Let $H1$ be a proper prefix of H. By PLD.4, PLD.3, PLD.2 worksOn($P, H1$). By AC.2, sameMotion($H1, HT, \{O\}, D$) and throughoutxSE($H1$,grasping(O)). By continuity (K.5) placement(O) is the same in end(H) as in end(HT); thus sameMotion($H, HT, \{O\}, D$). By DYN.11 there exists HX such that sameUntilEnd(HX, H) and holds(HX,grasping(O)). By AC.2, worksOn(move(O, HT),HX). By PLD.2, PLD.5, PLD.6, continuableEnd(P, H).

Therefore, we have begins(P, H) and $\neg$continuable(P, H). By PLD.3, PLD.4, PLD.5 baseExec$(P, H1)$ holds over every proper prefix $H1$ of J, but there is no proper extension $H2$ of J such that begins$(P, H2)$.

Suppose that parallelMovable$(O, \textit{end}(\text{H}), HT, \text{endTime}(H))$. Let HP, U satisfy the conditions of definition 2.13.B. Clearly HP satisfies the conditions on HK in DYN.14. Let $H2$ satisfy the conclusion of DYN.14. Using T.5, let $H3$ be the splicing of $H1$ followed by $H2$. By DYN.6, dynamic$(H3)$. It is immediate by construction that sameMotionOn$(H3, HT, \{0\}, D)$, and by DYN.14 throughoutxSE$(H3,\text{grasping}(O))$, hence beginsxE(move(O, HT),$H3$). But then if $H4$ is an extension of H and a proper prefix of $H3$, we have begins(move(O, HT),$H4$), so continuable(move(O, HT),H), which is a contradiction.

▮

Definition 2.14:
swathe(PS: pointSet; D: distance; $\hat{V}$: vector) $\rightarrow$ pointSet.
$P \in \text{swathe}(PS, D, \hat{V}) \Leftrightarrow \exists_{P1 \in PS, D1}\ 0 \leq D1 \leq D \wedge P = P1 + D \cdot \hat{V}$.

Definition 2.15:
lineTranslation(O:object, H:history, D: distance, V:vector) $\equiv$
$\forall_{T1,T2,S1,S2}\ T1 < T2 \wedge \text{stateAt}(H, T1, S1) \wedge \text{stateAt}(H, T2, S2) \Rightarrow$
$\exists_{D1}\ 0 < D \leq D1 \wedge \text{value}(S2,\text{placement}(O)) = \text{value}(S1,\text{placement}(O)) + D1 \cdot \hat{V}$.

Lemma 2.16:
$\text{lineTranslation}(O, H, D, V) \wedge \text{stateAt}(H, T, S) \wedge \text{convex}(R) \wedge$
$\text{value}(\text{start}(H),\text{place}(O)) \subset R \wedge \text{value}(\text{end}(H),\text{place}(O)) \subset R \Rightarrow$
$\text{swathe}(\text{value}(\text{start}(H),\text{place}(O)),D, V) \subset R$.

Proof: Immediate from 2.14, 2.15, definition of convexity. ▮

Definition 2.17:
horizontalVec(V: vector) $\equiv \forall_P\ \text{height}(P + V) = \text{height}(P)$.

Definition 2.18:
loadingTrajectory$(O, H) \equiv$
$\exists_{H1,H2,H3,D1,D2,D3,V}\ \text{hsplice}(H1, H2, H3, H) \wedge \text{lineTranslation}(O, H1, D1, \vec{z}) \wedge$
$\text{lineTranslation}(O, H3, D3, -\vec{z}) \wedge \text{lineTranslation}(O, H2, D2, V) \wedge \text{horizontalVec}(V) \wedge$
$\text{height}(\text{bottom}(O),\text{start}(H2)) > \text{value}(\text{start}(H),\text{top}^{\#}(\uparrow\text{oBox})) \wedge$
$\text{throughout}(H,\uparrow O \subset^{\#}\text{manipSpace1})$.

Lemma 2.18.1:
$\forall_{O \in \text{uCargo}}\ \text{holds}(\text{s1},\text{rccC}^{\#}(\uparrow O, \uparrow\text{oTable1}))$

Proof: From PR.11, H.1, HD.3, HD.1.

Lemma 2.18.2: $\forall_{O \in \text{uCargo}}\ \text{holds}(\text{s1},\text{bottom}^{\#}(O) \leq^{\#} \text{top}^{\#}(\text{oTable1}))$

Proof: From 2.18.1.

Lemma 2.18.3:
$\text{holds}(\text{s1},\text{top}^{\#}(\uparrow\text{qInsideBox}) \leq \text{top}^{\#}(\uparrow\text{oBox})$.

Proof: Geometric from PR.4, PR.9, SD.1 (EXPAND?) ‘

Lemma 2.19:
$\forall_{SA,SB,O,M}\ O \in \text{uCargo} \wedge \text{value}(SA,\text{placement}(O)) = \text{value}(\text{s1},\text{placement}(O)) \wedge$
$\text{value}(SA,\text{placement}(\text{oBox})) = \text{value}(SB,\text{place}(\text{oBox})) = \text{value}(\text{s1},\text{placement}(\text{oBox})) \wedge$
$\text{holds}(SB,O \subset^{\#} \uparrow\text{qInsideBox}) \wedge$
$\text{translation}(M) \wedge \text{imageMapping}(M,\text{value}(SA,\text{placement}(O)) = \text{value}(SB,\text{placement}(O)) \Rightarrow$
$\exists_H\ \text{loadingTrajectory}(O, H) \wedge \text{start}(H){=}SA \wedge \text{end}(H){=}SB$.

Proof: Bottom(O) is lower than top(oBox) in SA, by lemma 2.18.2, PR.17, and in SB by both SA and SB.
Let DH=(value(s1,top(oBox)) + top(manipSpace1) − maxCargoHeight)/2.
Let $H1$ be such that lineTranslation($O, H1, DH-$value(SA,bottom(O)),$\hat{z}$).
Let $H3R$ be such that lineTranslation($O, H3R, DH-$value(SB,bottom(O)),$\hat{z}$).
Let $H3$ be the time reversal of $H3R$, placed at a time interval after endTime($H1$).
By definition 2.15 value(end($H1$),bottom(O)) = value(start($H3$),bottom(O)) = DH.
Let $H2$ be the linear translation of O from end($H1$) to start($H3$); it is immediate that the rigid motion involved is translation, and that it is horizontal. Let H be the splicing of $H1$, $H2$, $H3$. The existence of histories $H1$, $H2$, $H3$ and H is guaranteed by axiom HC.2.

Let DG= (top(manipSpace1) − (value(s1,top(oBox)) + maxCargoHeight)) / 2 > 0 by PR.17.
By PR.16 value(end($H1$),top(O)) ≤ value(end($H1$),bottom(O)) + maxCargoHeight =
DH+maxCargoHeight = top(manipSpace1) − DG < top(manipSpace1).
Also value(end($H1$),bottom(O)) = DH = value(s1,top(oBox)) + DG >
value(s1,top(oBox)).

By PR.19, O is inside manipSpace1 throughout $H1$. It is easily shown from PR.4 and PR.10 that any point above any subset of qInsideBox is above oBox; hence O is inside manipSpace1 throughout $H3$. Finally using lemma 2.16 and axom PR.18 it is easily shown that O is inside manipSpace2 throughout $H2$.

∎

Lemma 2.20:
holds(start(H),midLoadingPosition) ∧ O ∈value(start(H),unloadedCargo) ∧
holds(end(H),boxLoadingPos(O,qInsideBox)) ∧ loadingTrajectory(O, H) ∧
$[\forall_{O1}\ O1 \neq O \Rightarrow$ motionless($H, O1$)] ⇒
moveTrajectory($H, O, \emptyset$,start(H),manipSpace1).

Proof: By definition 2.18, O is inside manipSpace1 throughout H. By PR.34, it does not overlap any object not in u1 ∪ { oTable1 }. Let H be decomposed into upward motion $H1$, horizontal motion $H2$, and downward motion $H3$ as in definition 2.18. By definition 2.2 and PR.14, no object in u1 comes into contact with O during $H1$. By PR17.5 and definition 2.18, no object in u1 ∪ { oTable1 } comes into contact with O during $H2$, because the objects in o1 are all lower than the top of oBox and O is higher than the top of oBox. By P1.4, P1.3 the swathe from O's position at end(H) upward to the top of manipSpace1 is clear of other objects in u1; hence no object comes into contact with O during $H3$. Hence all the conditions of moveTrajectory in P1.5 are met. ∎

Lemma 2.21 deliberately omitted.

Lemma 2.22:
[holds(S,midLoadingPosition) ∧ O ∈value(S),unloadedCargo)] ⇒
$\exists_H$ loadBoxConditions(O, H,unloadedCargo, qInsideBox,manipSpace1,S)

Proof: Immediate from axioms P1.9, definition 2.18, lemmas 2.12, 2.19, 2.20. ∎

Lemma 2.23:
holds(S,midLoadingPosition) ∧ value(S,unloadedCargo) ≠ ∅ ⇒
beginnable(loadBox(unloadedCargo,qInsideBox,manipSpace1),S).

Proof: Immediate from Lemma 2.22, axiom P1.10. ∎

Lemma 2.24:
$\forall_O\ O \in$ uCargo ∪ {oTable1} ⇒ holds(s1,rccDC$^{\#}$(↑O,↑qInsideBox)).

Proof: Immediate from corollary 2.11.A, PR.13.

Lemma 2.25:
worksOn(move(O, HT),H) $\Leftrightarrow$
$\exists_D$ D =startTime(H)$-$startTime(HT) $\land$
[endTime(H) $<$ endTime(HT) $\land$
$\exists_{H2}$ historyPrefix($H2, HT$) $\land$ sameMotionOn($H2, H, \{O\}, D$) $\land$ throughout(H,grasping(O))] $\lor$
[endTime(HT) $\leq$ endTime(H) $\land$
$\exists_{HA,HB}$ hsplice(HA, HB, H) $\land$ sameMotionOn($HA, HT, \{O\}, D$) $\land$
throughoutxSE(HA,grasping(O)) $\land$ throughout(HB,freeGrasp).

Proof: Immediate from axiom AC.2 by a simple temporal argument. ▮

Lemma 2.26:
beginnable(loadBox(U, QI, RM),start(H)) $\land$ attempts(loadBox(U, QI, RM),H) $\Rightarrow$
$\exists_{O,H2}$ loadBoxConditions($O, H2, U, QI, RM$) $\land$ attempts(move($O, H2$),H).

Proof: Assume that beginnable(loadBox(U, QI, RM),start(H)) and attempts(loadBox(U, QI, RM),H). By PLD.2–PLD.7, for any proper prefix $H1$ of H, worksOn(loadBox(U, QI, RM),$H1$). By P1.11 for any such $H1$ there exists $O, H1T$ such that loadBoxCondition($O, H1T, U, QI, RM$), worksOn(move($O, H1T$),$H1$). The difficulty at this point of the proof is that each such $H1$ may correspond to a *different* O and $H1T$; we need to show that there is a single O and $H1T$ that works for all such prefixes $H1$. There are two cases:

Case 1: For some such $H1$ and $H1T$, end($H1T$) $\leq$ end($H1$). By lemma 2.25, there exists HA, HB, D, such that hsplice($HA, HB, H1$), sameMotionOn($HA, H1T, \{O\}, D$), throughoutxE(HA,grasping(O)) and throughout(HB,freeGrasp). It is immediate from AC.2, DYD.4, DYD.2 that, for every proper prefix $H2$ of $H1$, worksOn(move($O, H1T$),$H2$).

By PLD.8 since attempts(loadBox(U, QI, RM),H) it must either be the case that $\neg$continuable(loadBox(U, QI, RM)) or that $\neg$continuableEnd(loadBox(U, QI, RM)). Since continuing working on loadBox(U, QI, RM) only involves maintaining freeGrasp, which is always dynamically possible (DYN.12, DYN.10, DYN.6), it must be the case that reactComplete(loadBox(U, QI, RM),H), which means that completion(loadBox(U, QI, RM),H) holds at endTime(H)$-$reactionTime. By P1.12, for some HX, loadBoxCondition(O, HX, U, QI, RM) and completion($H2$,move(O, HX),H); by AC.3, for some D, sameMotionOn($HX, H, \{O\}, D$). By the above argument for every proper prefix $H3$ of H, workOn(move(O, HX),$H3$) and $\neg$reactComplete(move(O, HX),$H3$). Hence attempts(move(O, HX),H).

Case 2: For all such $H1$ and $H1T$, end($H1$) $<$ end($H1T$). Define the formula $\Psi(O1, T, M, HX, OX)$ as follows:

$$[O1 = OX \Rightarrow \exists_S \text{ stateAt}(HX, T, S) \land M{=}\text{value}(S,\text{placement}(OX))] \land$$
$$[O1 \neq OX \Rightarrow M{=}\text{placement}(\text{start}(HX),O1)]$$

It is immediate that for $HX = H$, $OX = O$, the formula Ψ defines a unique mapping and satisfies the Lipschitz condition throughout the time interval from start(H) to end(H). Hence by axom HC.2 there exists a history $H2$ corresponding to Ψ. Using the construction in lemma 2.19, let $H3$ be a trajectory that translates O from its position at end($H2$) to a position satisfying boxLoadingPos(O, QI). Let $H3$ be the splice of H followed by $H2$. It is easily verified that loadBoxConditions($O, H3, U, QI, RM$), and that for every prefix $H4$ of H, worksOn(move($O, H3$),$H4$).

By PLD.4 since attempts(loadBox(U, QI, RM),H) it must be the case that either $\neg$continuableEnd(loadBox(U, QI, RM),H) or $\neg$continuable(loadBox(U, QI, RM),H). By DYN.11 there exists a history $H1$ which is identical to H up until its end and for which holds(end($H1$),grasping(O)). By continuity (K.5), the position of O at endTime(H) must be the same in $H1$, H, and $H1T$. Therefore baseExec(loadBox(U, QI, RM),$H1$), hence by PLD.5, continuableEnd(loadBox(U, QI, RM),H).

The remaining possibility is $\neg$continuable(loadBox(U, QI, RM)). Since the condition for loadBox(U, QI, RM) is certainly not satisfied in H, it must be the case that there is no extension HE of H such that worksOn(loadBox(U, Q, RM),HF) is dynamically possible for every prefix HF of HE. In particular, this must hold for all the extensions HE that correspond to the continued execution of move($O, H3$). Thus, we have established that worksOn(move($O, H3$),$H4$) is achieved for every prefix $H4$ of H and is not achievable throughout any extension $H4$ of H; hence attempts(move($O, H3$),H).

∎

Lemma 2.27:
holds(start(J),midLoadingPosition) $\wedge$ value(start(J),unloadedCargo) $\neq \emptyset$ $\wedge$
holds(start(J),stable(u1 $\cup$ { oTable1 }) $\wedge$ isolationConditions(J,problem1) $\wedge$
attempts(loadBox(unloadedCargo,qInsideBox,manipSpace1),J)
$\Rightarrow$
completes(loadBox(unloadedCargo,qInsideBox,manipSpace1),J) $\wedge$
$\exists_{O,H2,S2}$ completes(move($O, H2$),J) $\wedge$
loadBoxConditions($O, H2$,unloadedCargo,qInsideBox,manipSpace1) $\wedge$
stateAt(J,endTime($H2$),$S2$) $\wedge$ sameStateExcept($S2$,start(J),$\{O\}$) $\wedge$
holds($S2$,boxLoadingPos(O,qInsideBox)).

Proof: By lemma 2.23, beginnable(loadBox(unloadedCargo,qInsideBox,manipSpace1),start(J)). By lemma 2.26, there exist $H2$ and O such that loadBoxConditions($O, H2$,unloadedCargo,qInsideBox,manipSpace1) and attempts(move($O, H2$),J). It follows from lemma 2.26 that J is bounded.

By lemma 2.25, throughout J the agent is either grasping O or has a free grasp; therefore he is never grasping any object in u1 other than O (G.1).

Let $J2$ be the prefix of J with endTime($J2$)=endTime($H2$); that is, the part of J in which O is carrying out the motion in $H2$ and excluding any part of J after the motion is complete waiting for reactionTime to pass. Let UUN=value(start(J),unloadedCargo)$-\{O\}$ and ULD=value(start(J),loadedCargo). We claim the following is true:

CLAIM.1:
[$\forall_{O1}$ $O1$ $\in$u1$-\{O\}$ $\Rightarrow$ motionless($J2, O1$)] $\wedge$
[$\forall_{O1}$ $O1 \in UUN$ $\Rightarrow$
throughoutxSE($J2$,isolated($\{O1\}$, { oTable1 }) $\wedge$
throughoutxSE($J2$,isolated($ULD \cup$ { oBox }, { oTable1 }))

The proof of CLAIM.1 is by contradiction: We posit that CLAIM.1 becomes false at some point, consider the greatest lower bound $T0$ of the times on which it is false, and show that if CLAIM.1 is true until $T0$ then it continues to be true both at $T0$ and for some time afterward. Specifically: Suppose that CLAIM.1 is false. Define the formula $\Phi(T)$ as follows.

$\Phi(T) \equiv$
$\exists_S$ stateAt(J, T, S) $\wedge$
[[$\exists_{O1 \in \text{u1}-\{O\}}$ value(S,placement($O1$)) $\neq$ value(start(J),placement($O1$)] $\vee$
[$\exists_{O1,O2}$ $O1 \in UUN \wedge O2 \neq$oTable1 $\wedge$ $O2 \neq O1$ $\wedge$ holds(S, rccC$^{\#}$($\uparrow O2, \uparrow O1$))] $\vee$
[$\exists_{O1,O2:\text{object}}$ $O1 \in ULD \cup$ { oBox } $\wedge$ $O2 \notin ULD \cup$ { oBox, oTable1} $\wedge$ holds(S, rccC$^{\#}$($\uparrow O2, \uparrow O1$))]

If CLAIM.1 is false, then $\Phi(T)$ must hold for some T such that startTime(J) $\leq T <$endTime($J2$). Let $T0$ be the greatest lower bound on all times on which Φ holds. Since $O1$ remains at the same position as in start(J) up until $T0$, it follows by continuity (K.5) that it is in the same position in $T0$. By definition 2.2, oBox and the cargo objects that are unloaded at start(J) are all in the same position as in s1; hence, by PR.12 none of these are touching one another. By definition the loaded cargo objects are inside qInsideBox; hence, by lemma 2.24, none of the unloaded objects are touching any loaded objects. By PR.33 any object that is not in u1 and is not oTable1 is outside manipSpace1 and hence is not in contact with any of the objects in u1. By P1.8, O itself is not in contact with any objects in u1 during J. Therefore in start(J) each of the unloaded cargo objects is isolated except for oTable1 and the loaded cargo plus box is collectively isolated except for oTable1. Since the cargo objects and box remain motionless from start(J) through $T0$, these isolation conditions hold at $T0$.

Since each unloaded object is a finite distance from every other object except oTable1, and since the loaded cargo objects plus box are a finite distance form every other object except oTable1, by continuity, a finite time must pass until any of these excluded contacts occur. Thus, these isolation conditions must in fact hold over the interval from start(J) to $T1$ where $T1 > T0$.

By assumption, the objects in u1 are all in stable positions at start(J); hence by H.2 all the objects except O are in the identical stable positions at $T0$. Hence by axiom H.2, the objects in u1 remain motionless over the entire interval from start(J) to $T1$. By the identical argument as above, the isolation conditions likewise hold over the entire interval from start(J) to $T1$; but that contradicts the construction of $T0$. This completes the proof of CLAIM.1.

Suppose that the action move($O, H2$) does not complete in J. Then endTime(J) = endTime($H2$) = endTime($J2$) By lemma 2.13 ¬parallelMovable(O,end(J),$H2$,endTime($H2$); however, by P1.5, before the end of $H2$, O is in fact isolated from all other objects, so parallelMovable is satisfied trivially, with $U1 = \{O\}$ and HP being the history in which O follows $H2$ and all other objects remain motionless. This is a contradiction; therefore, move($O, H2$) does complete in J. By P1.8, P1.9, P1.10 it follows directly that completes(loadBox(unloadedCargo,qInsideBox,manipSpace1),JP).

▮

Lemma 2.28
$\forall_{OB,OC\text{:object},QI,QTOP,QPC\text{:pseudo},H\text{:history}}$
openBox($OB, QI, QTOP$) ∧ OB = source(QI) = source($QTOP$) ∧
source(QPC)=OC ∧ point(QPC) ∧ $QPC \in OC$ ∧
holds(start(H),$\uparrow QPC \in^{\#} \uparrow QI - \uparrow QTOP$) ∧ ¬holds(end($H$),$\uparrow QPC \in^{\#} \uparrow QI$) ⇒
$\exists_{T,S}$ stateAt(H, T, S) ∧ holds(S,$\uparrow QPC \in^{\#} \uparrow QTOP$).

Proof: Let us first consider the case where shape(QPC) is a point in the interior of OC. Since QPC and QIN both move continuously, and QPC goes being in QI to being outside QI, it must at the boundary of QI at some state S in between. By SP.1, QPC is either at the boundary of OB or in $QTOP$.

Suppose that QPC is at the boundary of OB in S. Since QPC is in the interior of shape(OC), there exists an open neighborhood RC of value(S,place(QPC)) which is a subset of value(S,place(OC)). in (QPC) $\in RC \subset OC$. Since OB is regular, there exists an open set RB ⊂value(S,place(OB)) such that value(S,place(QPC)) is in the closure of RB. But then RB and RC must overlap and so must OB and OC, which is impossible since S is kinematic.

Suppose now that shape(QPC) is a point on the boundary of OC. Since OC is regular, there exists an open set $RC \subset$ shape(OC) such that shape(QPC) ∈ boundary(RC). Suppose that QPC is never in $QTOP$ during H. Since $QTOP$ is topologically closed, there must exist a positive minimum distance D such that distance($QPC, QTOP$) is at least D throughout H. But that is impossible, since by the previous argument every point in interior(OC) is in $QTOP$ at some time in H, and there are points in interior(OC) that are arbitrarily close to QPC.

▮

Lemma 2.29

$\forall_{OB,OC:\text{object},QI,QTOP:\text{pseudo},H:\text{history}}$
openBox($OB, QI, QTOP$) $\wedge$ OB = source(QI) = source($QTOP$) $\wedge$
kinematic(H) $\wedge$ holds(start(H),$\uparrow OC \subset^{\#} \uparrow QI$) $\wedge$ holds(end(H),$\neg^{\#}[OC \subset^{\#} QI]$) $\wedge$ [motionless(H, OB)
$\vee$ goodBoxTrajectory($H, OB, QIN, QTOP, \{O\}$)] $\Rightarrow$
$\exists_{H1}$ historyPrefix($H1, H$) $\wedge$ upwardMotion($O, OB, H1$)

Proof: First, a simple trigonometric formula: let PA and PB be any two points and let Q be a coordinate system whose z axis is angle θ away from the vertical. Then
zCoor(PA, Q)$-$zCoor(PB, Q) $\geq$
(height(PA)$-$height(PB)) cos(θ) $-$ distance(xyProj(PA),xyProj(PB))sin(θ).

Using CM.1, let QPC be any point in OC. By lemma 2.28 there is a state S at some time $T1$ in H at which QPC is in $QTOP$. Let $H1$ be the prefix of H ending at $T1$. Let T be any time between startTime(H) and $T1$; let ST be the state of H at T; let QCS be a coordinate system attached to oBox whose z axis is vertically aligned in start(H), and let QCT be a coordinate sytem attached to oBox whose z axis is vertically aligned in ST By P1.16, if goodBoxTrajectory($H, OB, QIN, QTOP, \{O\}$) then the angular difference θ between the z axis of QCT and the z axis of QCS satisfies safeBoxTilt(θ,start(H),$QIN, QTOP, O$); if motionless(OB, H) then $\theta = 0$.

Now, let QPT be the pseudo-object such that source(QPT)=oBox and value(end($H1$),place(QPT)) = value(end($H1$),place(QPC)). Note that shape(QPT) $\in$ shape($QTOP$).
Let $PM1$=value(start(H),centerMass(O)); $PC1$=value(start(H),place(QPC));
$PT1$=value(start(H),place(QPT)); $PC2$=value(end($H1$),place(QPC));
$PT2$=value(end($H1$),place(QPT)); and $PM2$=value(end($H1$),centerMass(O).

Thus we have the following constraints:
zCoor($PM2, QCT$) $\geq$ zCoor($PC2, QCT$)$-$diameter(O) by lemma CM.1.
$PT2 = PC2$ by construction.
zCoor($PT1, QCT$) = zCoor($PT2, QCT$), since QPT and QCT both move with oBox.
zCoor($PT1, QCT$) $-$ zCoor($PM1, QCT$) $\geq$
(height($PT1$)$-$height($PM1$)) cos(θ) $-$ distance(xyProj($PT1$),xyProj($PM1$))sin(θ).

Therefore zCoor($PM2, QCT$)$-$ zCoor($PM1, QCT$) $\geq$
(height($PT1$)$-$height($PM1$)) cos(θ) $-$ distance(xyProj($PT1$),xyProj($PM1$))sin(θ) $-$ diameter(O).

Since $PM1$ $\in$value(start(H),QIN) and since $PT1$ $\in$value(start(H),$QTOP$), it follows that distance(xyProj(PA),xyProj(PB)) $\leq$ diameter(xyProj($QIN \cup QTOP$)).
Moreover if bottom1(value(S,place($QTOP$)),$D1$) then height($PT1$) $\geq$ $D1$.

Hence, by P1.16, P1.17 zCoor($PM2, QCT$)$-$ zCoor($PM1, QCT$) > 0, so by UD.1 O undergoes an upward motion relative to { oBox } in $H1$.

∎

Lemma 2.30:

P= sequence(loadBox(unloadedCargo,qInsideBox,manipSpace1),J),
waitUntil(stable(u1 $\cup$ { oTable1 }))) $\wedge$
UUL=value(start(J),unloadedCargo) $\neq \emptyset$ $\wedge$
holds(start(J),midLoadingPosition) $\wedge$ holds(start(J),stable(u1 $\cup$ { oTable1 }) $\wedge$
noAnomaly2(J) $\wedge$ noAnomUpwardMotion(J) $\wedge$ throughout(J,isolFluent(problem1)) $\wedge$
attempts(P, J)
$\Rightarrow$

completes(P, J) ∧ holds(end(J),midLoadingPosition) ∧
$\exists^1_{O \in UUL}$ value(end(J),unloadedCargo) = $UUL - \{O\}$.

Proof: By lemmas 2.27 and 1.21 there exist $H1, J2$ such that J is the splice of HA and JB, the loadBox completes in HA, freeGrasp holds throughout $J2$ and either waitUntil(stable(u1 ∪ { oTable1 })) completes in $J2$ or $J2$ is unbounded and stable(u1 ∪ { oTable1 }) is forever false.

Using the conclusions of lemma 2.27 let O be the object that was loaded into the box and let $H2$ be the trajectory of motion, and let $S2$ be the state of J at endTime($H2$). By lemma 2.27, holds($S2$,loadingPos(O)). As in the proof of lemma 2.27, let ULD=value(start(J),loadedCargo) and let UUN=value(start(J),unloadedCargo).

By P1.7 O is in contact, either with oBox or with one of the other loaded cargo objects. Note that value(end($J2$),loadedCargo)=$ULD \cup \{O\}$.

Let $J3$ be the slice of J from endTime($H2$) to endTime(J). Thus $J3$ consists of the splice of the end of HA, in which the movement of O has finished and the agent is waiting for reactTime to pass for the action to be complete, followed by JB in which the agent is waiting for the objects u1 ∪ oTable1 to attain a stable state. Note that in both of these parts of $J3$ the agent is not grasping anything. We now make a claim about the behavior of the objects in $J3$:

CLAIM.2:
[$\forall_{O1 \in UUN}$ motionless($J3, O$) ∧ throughout($J3$,isolated($\{O1\}$, {oTable1}) ∧
throughout($J3$,isolated($ULD \cup \{O,$ oBox$\}$, { oTable1 }) ∧
motionless($J3$,oBox) ∧
$\forall_{O1 \in ULD \cup \{O\}}$ throughout(J,$\uparrow O \subset^\# \uparrow$qInsideBox).

The structure and many of the details of the proof of CLAIM.2 is the same as for CLAIM.1. Suppose that CLAIM.2 is false. Define the formula $\Phi(T)$ as follows.

$\Phi(T) \equiv$
$\exists_S$ stateAt($J3, T, S$) ∧
  [[$\exists_{O1 \in UUN}$ ∧ value(S,placement($O1$)) ≠ value(start($J3$),placement($O1$)] ∨
  value(S,placement(oBox)) ≠ value(start($J3$),placement(oBox)) ∨
  [$\exists_{O1,O2}$ $O1 \in UUN$ ∧ $O2 \neq$oTable1 ∧ $O2 \neq O1$ ∧ holds(S, rccC$^\#$($\uparrow O2, \uparrow O1$))] ∨
  [$\exists_{O1,O2}$ $O1 \in ULD$ ∪ { oBox } ∧ $O2 \notin ULD$∪ { oBox, oTable1} ∧
    holds(S, rccC$^\#$($\uparrow O2, \uparrow O1$))] ∨
  [$\exists_{O1 \in ULD \cup \{O\}}$ ¬holds(S,$\uparrow O \subset^\# \uparrow$qInsideBox)]
  ].

Suppose that $\Phi(T)$ holds for some T; let $T0$ be the greatest lower bound over times on which Φ holds. By continuity, all the objects in UUN and oBox are still in the same position in $T0$ as in start($J3$), and the objects in ULD are still inside qInsideBox. The argument that the isolation conditions still hold in $T0$ and therefore until some time $T1 > T0$ is the same as in the proof of CLAIM.1 above.

Let $J4$ be the prefix of $J3$ ending at $T1$. By HD.6 and UD.3, ¬anomaly2($J4$) and ¬anomalousUpwardMotion($J4$). By axiom PR.11, in start($J4$) the condition of HD.5, that oBox is stably supported by oTable1 ignoring the loaded cargo objects, is satisfied. Therefore all the conjuncts in the definition of anomaly2($J4$) are satisfied except possibly ¬throughout($J4$, motionless(OB)). Since ¬anomaly2($J4$), it follows that throughout($J4$, motionless(OB)).

Since the objects in ULD are in the same positions in start($J3$) as in start(J) and since in start($J3$) O is in contact either with one of the objects in ULD or with oBox, it follows from HD.3 that all of the objects in $ULD \cup \{O\}$ are in a heap supported by oBox. Since oBox is motionless throughout $J4$, any coordinate system aligned with oBox at any time throughout $J4$ has a vertical z-axis throughout $J4$. By UD.2, UD.1, none of the objects in $ULD \cup \{O\}$ increase their z-coordinate with respect to oBox during $J4$. Therefore, by lemma 2.29, they all remain inside the box. Thus, all of the conditions of $\Phi(T)$ are satisfied at least until time $T1$; but that contradicts the construction of $T0$. This completes the proof of CLAIM.2.

Using the same argument as in the previous paragraph, it follows that no object in $ULD \cup \{O\}$ has its center of mass rise during $J3$. Hence boxLoadingPos still holds at the end of $J3$.

It follows from lemma 2.3 that waitUntil(stable(u1 $\cup$ {oTable1})) completes in JB. Hence, it follows from lemma CS.8 that completes(P, J). The conditions in definition 2.2 for holds(end(J),midLoadingPosition) have all been established above.

▮

Define the following constant:

loadLoop=
while(unloadedCargo $\neq^{\#} \emptyset$,
    sequence(loadBox(unloadedCargo,qInsideBox,manipSpace1),
        waitUntil(stable(u1 $\cup$ { oTable1 })))).

Lemma 2.31:
start(J)=s1 $\wedge$ attempts(loadLoop,J) $\wedge$
isolationCondition(J,problem1) $\wedge$ noAnomaly2(J) $\wedge$ noAnomUpwardMotion(J)
    $\Rightarrow$
completes(loadLoop,J) $\wedge$ holds(end(J),midLoadingPosition) $\wedge$
$\forall_{O \in \text{uCargo}}$ holds(end(J), $O \subset$qInsideBox)

Proof: From 1.30, where the loop invariant $\Phi(S)$ is holds(S,midLoadingPosition), together with lemma 2.30 and lemma 1.31. The conclusion that all the cargo object end up in the box follows from the fact that it is easily shown that the formula value(S,unloadedCargo) $\cup$ value(S,loadedCargo) = u1 is a loop invariant, and that value(S,unloadedCargo)=$\emptyset$ at the end of the loop. ▮

3 Carrying

Let H be any history such that start(H)=s1, isolationCondition(H,problem1), and completes(loadLoop,H). Let sLoaded=end(H).

Let pCarry=carryBox(oBox,qInsideBox,qTopBox,uCargo,oTable2,manipSpace2)

Lemma 3.1:
carryBoxConditions(carryingPath,oBox,qInside,qTop,uCargo,manipSpace2,oTable2, sLoaded).

Proof: Immediate from axioms PR.25 through PR.32. Note that by PR.32, the vertical tilt of the box throughout carryingPath is zero. Therefore the condition in goodBoxTrajectory becomes that the height difference between qTop and the center of mass of any of the cargo objects O is at least diameter(O), but this is guaranteed by the fact that midLoadingPosition holds in sLoaded (lemma 2.31). ▮

Lemma 3.2:
beginnable(pCarry,sLoaded).

Proof: Immediate from P1.16, lemma 3.1. ▮

Lemma 3.3:
beginnable(pCarry,start(H)) $\wedge$ attempts(pCarry,H) $\Rightarrow$
$\exists_{O,H2}$ carryBoxConditions($H2$,oBox,qInside,qTop,uCargo,manipSpace2,oTable2, sLoaded) $\wedge$
attempts(move(oBox,$H2$),H).

Proof: Exactly analogous to the proof of 2.26. ∎

(Presumably both lemma 3.3 and lemma 2.26 are instances of some more general meta-level lemma about plans that are instantiated as moves satisfying certain kinds of conditions, but I have not attempted to formulate this.)

Lemma 3.4:
$\forall_{O \in \text{uCargo}} \exists_{UH}\ O \in UH \wedge$ holds(sLoaded,heap(UH,{oBox})).

Proof: Since the cargo objects are all inside qInsideBox in s1, by PR.33, PR.19 they are not touching any object other than oTable1 and oBox and by lemma 2.24 they are not touching oTable1; thus, the cargo objects are only touching one another and oBox. Let O be a cargo object. Since u1 $\cup$ oTable1 is stable in sLoaded, by HD.4, H.1 O is part of some heap UH that is supported by a set US of objects not free to move. There are two cases:

- Case 1: The agent is grasping oBox in sLoaded. Then since all the objects in uCargo are free, US must consist of objects not in uCargo. Since the only object not in uCargo that any object in uCargo is touching is oBox, by HD.3 UH = { oBox }.
- Case 2: The agent is not grasping oBox in sLoaded. Then since all the objects in u1 are free, US must consist of objects not in u1. (Actually, of course US = { oTable1 }, but we will not need that here.) Since oBox is the only object in u1 that is touching any object not in u1, by HD.3, oBox is in UH. Let $UH1$ be the maximal connected group of objects in uCargo containing O. Since $UH1$ is maximal, and since the objects in uCargo are separated from every object not in uCargo except oBox, by HD.1, HD.3, $UH1$ is a heap with support { oBox }.

∎

Lemma 3.5:
start(J)=sLoaded $\wedge$ throughout(J,isolFluent(problem1)) $\wedge$ noAnomaly2(J) $\wedge$
noAnomUpwardMotion(J) $\wedge$ attempts(pCarry,J)
$\Rightarrow$
completes(pCarry,J) $\wedge$
$\exists_{O,H2,S2}$ completes(move($O, H2$),J) $\wedge$
carryBoxConditions($H2$,oBox,qInside,qTop,uCargo,manipSpace2,oTable2, sLoaded) $\wedge$
stateAt(J,endTime($H2$),$S2$) $\wedge$
$\forall_{O \in \text{uCargo}}$ holds($S2, O \in$qInsideBox).

Proof: (Note: This is analogous to the proof of lemma 2.27, though certainly different in detail.)

By lemma 3.2, beginnable(pCarry,sLoaded). By lemma 3.3 there exists $H2$ such that carryBoxConditions($H2$,oBox,qInside,qTop,uCargo,manipSpace2,oTable2, sLoaded) and attempts(move(oBox,$H2$),H).

I claim that the following holds:

CLAIM.3:
throughout(H,isolated(u1,{oTable1, oTable2}) $\wedge$
$\forall_{O \in \text{uCargo}}$ throughout(H,$\uparrow O \subset^{\#} \uparrow$qInsideBox)

The proof of CLAIM.3 is by contradiction. Suppose it is false. Let $\Phi(T)$ be the formula

$\Phi(T) \equiv$
$\exists_S$ stateAt$(H,T,S) \wedge$
$[\ [\exists_{O1,O2:\text{object}}\ O1 \in \text{u1} \wedge \text{O2} \notin \text{u1} \cup \{\ \text{oTable1, oTable2}\ \} \wedge \text{holds}(S\text{rccEC}^{\#}(\uparrow O1, \uparrow O2))] \vee$
$[\exists_{O1 \in \text{uCargo}}\ \neg\text{holds}(S, O1 \subset \text{qInsideBox})]]$.

If CLAIM.3 is false, then $\Phi(T)$ must hold for some T. Let $T0$ be the greatest lower bound on all times T such that Φ holds. By continuity, the objects in u1 remain separated from any object not in u1 $\cup$ { oTable1, oTable2 } up through some time $T1 > T0$. Since the agent is grasping oBox throughout H, by G.1 he does not grasp any object in uCargo at any time in H. By lemma 3.4 the cargo objects are in heaps supported by oBox in sLoaded. By lemma 2.29, UD.3, UD.2, the objects in uCargo all remain inside the box though time $T1$; but this contradicts the construction of $T0$. This completes the proof of CLAIM.3

Suppose that the action move(oBox,$H2$) does not complete in J. Then endTime(J) = endTime($H2$) = endTime($J2$) By lemma 2.13, at end(J), ¬ parallelMovable(oBox,end(J),$H2$,endTime(J)). However, throughout J the cargo is isolated from any object except oBox, and oBox is isolated from any objects except oTable1 and oTable2. Moreover, the continuation of $H2$ does not bring oBox into contact with any objects except oTable2 at the end of H. Therefore, the history that moves oBox along the continuation of $H2$ and moves all of the cargo in parallel and keeps everything else motionless is kinematically possible. The existence of this history is guaranteed by HC.2. Note that it is easily shown that qInsideBox lies inside the convex hull of oBox. Since all the points in oBox are moving no faster than maxSpeed (HC.1), any point inside the convex hull of oBox is likewise moving no faster than maxSpeed. Thus all the conditions of parallelMovable in definition 2.13.B are met, which is a contradiction.

Thus, move$(O, H2)$ does complete in J. By PL.19–PL.22 it follows that pCarry completes in J.

▮

Definition 3.6.A holds(S,goalState) $\equiv \forall_{O \in \text{uCargo}}$ holds(S,altogetherAbove(O,oTable2)/

Lemma 3.6:
start(J)=sLoaded ∧ completes(pCarry,J) ∧
throughout(J,isolFluent) ∧ noAnomaly2(J) ∧ noAnomUpwardMotion(J) ⇒
holds(end(J),goalState).

Proof: Let $H2$ be as in Lemma 3.5. By lemma 3.5, all the cargo objects are inside qInsideBox in J at time endTime($H2$). By an argument exactly analogous to the proof of lemma 16, the objects remain inside qInsideBox during the "reaction" interval between endTime($H2$) and endTime(J). by P1.15 and a simple geometric argument, all the objects in uCargo are above oTable2 at end(H). ▮

Lemma 3.7:
start(J)=s1 ∧ attempts(plan1,J) ∧
throughout(J,isolFluent) ∧ noAnomaly2(J) ∧ noAnomUpwardMotion(J) ⇒
completes(plan1,J) ∧ holds(end(J),goalState).

Proof: From lemmas 1.21, 2.31, 3.2, and 3.6. ▮

Define the uhistory j1 to satisfy the following axiom:

J1.1 start(j1)=s1 ∧ attempts(plan1,j1).

Note that the existence of such a j1 is guaranteed by lemma 1.5.

Theorem 1:
isolationConditions(j1,problem1) ⇒ completes(plan1,j1) ∧ holds(end(j1),goalState).

Proof: It is easily seen that the propositions "noAnomaly2(j1)" and "noAnomUpwardMotion(j1)" are consistent with the our axioms and with Newtonian mechanics. (E.g. Consider the case where oBox is a rectangular box with a rectangular inside; the cargo objects are all rectangular cuboids; the cargo objects are loaded neatly in the box from bottom to top; and the box is moved smoothly and without tilting from oTable1 to oTable2.) Therefore, the default rules H.4 and UP.1 allow us to infer noAnomaly(j1) and noAnomUpwardMotion(j1). The result then follows from lemma 3.7. ∎

References

[1] E. Davis, "Knowledge and Communication: A First-Order Theory," *Artificial Intelligence,* vol. 166 nos. 1-2, 2005, pp. 81-140.