Proofs on expressing nested GR(1) properties in GR(1)

Ioannis Filippidis

ifilippi@caltech.edu

Control and Dynamical Systems
California Institute of Technology

December 22, 2017

Abstract

This is a proof that any nested GR(1) property is equivalent to a GR(1) property, by adding an auxiliary variable that counts up to the nesting depth, which is at most equal to the number of states. In practice the nesting depth is small.

The proof style below is described in [1]. The results are proved for stutter-sensitive properties, and stutter-sensitive temporal quantification ($\exists\!|, \forall\!|$). Wherever we invoke arguments about history-determined variables, these are analogous to the stutter-invariant case [2].

The rules of TLA$^+$ are assumed for declaring variables, so when writing $\exists\!| q : a$ in a theorem statement, the identifier q stands for a fresh name in the context where the theorem is applied. For this reason, where possible we do not mention assumptions about what identifiers can occur when.

ASSUME The operators take Boolean values, except where otherwise noted.

Definition 1 *Let* $d \in Nat, H_k \in Nat, \Xi_m \in Nat$. *A* chain condition *is a formula of the form:*

$$\begin{array}{lll} \wedge\, \forall m \in 1..d : & \wedge\, P_{m-1} \Rightarrow Q_m & \\ & \wedge\, \forall l \in 0..\Xi_m : \xi_{ml} \Rightarrow \neg P_{m-1} & \\ \wedge\, \forall m \in 0..d : & \wedge\, Q_m \Rightarrow P_m & \\ & \wedge\, \forall l \in 0..H_m : \eta_{ml} \Rightarrow (P_m \wedge \neg Q_m) & \\ & \wedge\, \forall l \in 0..\Xi_m : \xi_{ml} \Rightarrow Q_m & \end{array}$$

ASSUME *ChainCondition* $\triangleq$ The operators $P_m, Q_m, \xi_{ml}, \eta_{ml}$ satisfy a chain condition (Definition 1).

Definition 2 (Nested GR(1) property [3]) *Let*

$$\begin{array}{rcl} \varphi & \triangleq & \Box \bigwedge_{m \in 0..d} \wedge \vee \neg P_m \\ & & \qquad \vee \neg \bigwedge_{k \in m..d} \bigwedge_{l \in 0..H_k} \Box\Diamond \neg \eta_{kl} \\ & & \qquad \vee \Diamond Q_m \\ & & \qquad \wedge \left(Q_m \Rightarrow \bigwedge_{l \in 0..\Xi_m} \Box\Diamond \neg \xi_{ml}\right) \end{array}$$

φ *is a* nested GR(1) *property.*

A nested GR(1) property is defined here as a liveness formula. Inserting a liveness formula of this form in a stepwise implication operator ($\stackrel{+}{\triangleright}$, *WhilePlusHalf*, or some other choice) can yield an open-system property.

Proposition 3

$$\begin{array}{lll} \text{LET } \varphi_1 & \triangleq & \Box((\bigwedge_i \Box\Diamond A_i) \Rightarrow B) \\ \quad \varphi_2 & \triangleq & (\bigwedge_i \Box\Diamond A_i) \Rightarrow \Box B \\ \text{IN } \quad \varphi_1 \equiv \varphi_2 & & \end{array}$$

$\langle 1\rangle 1$. DEFINE $\varphi_1 \triangleq \Box((\bigwedge_i \Box\Diamond A_i) \Rightarrow B)$
$\qquad\qquad\quad \varphi_2 \triangleq (\bigwedge_i \Box\Diamond A_i) \Rightarrow \Box B$
$\langle 1\rangle 2$. SUFFICES
ASSUME NEW $\sigma, IsABehavior(\sigma)$
PROVE $\sigma \models \varphi_1 \equiv \varphi_2$
$\langle 1\rangle 3$. CASE $\sigma \models \bigwedge_i \Box\Diamond A_i$
$\langle 2\rangle 1$. $\sigma \models (\bigwedge_i \Box\Diamond A_i) \Rightarrow \Box(\bigwedge_i \Box\Diamond A_i)$
$\langle 2\rangle 2$. CASE $\sigma \models \neg\Box B$
$\langle 3\rangle 1$. $\sigma \models \Diamond\neg B$
BY $\langle 2\rangle 2$
$\langle 3\rangle 2$. $\sigma \models \Box \bigwedge_i \Box\Diamond A_i$
BY $\langle 1\rangle 3$, $\langle 2\rangle 1$
$\langle 3\rangle 3$. $\sigma \models \neg\varphi_1$
$(\Box \bigwedge_i \Box\Diamond A_i) \wedge \Diamond\neg B \equiv \Diamond\big(\neg B \wedge \bigwedge_i \Box\Diamond A_i\big) \equiv \neg\Box\big((\bigwedge_i \Box\Diamond A_i) \Rightarrow B\big)$
$\langle 3\rangle 4$. $\sigma \models \neg\varphi_2$
$\neg\Box B \wedge \bigwedge_i \Box\Diamond A_i \equiv \neg\big((\bigwedge_i \Box\Diamond A_i) \Rightarrow \Box B\big)$
$\langle 3\rangle 5$. QED
BY $\langle 3\rangle 3$, $\langle 3\rangle 4$
$\langle 2\rangle 3$. CASE $\sigma \models \Box B$
BY $\langle 2\rangle 3$ DEF φ_1, φ_2
$\langle 2\rangle 4$. QED
BY $\langle 2\rangle 2$, $\langle 2\rangle 3$
$\langle 1\rangle 4$. CASE $\sigma \models \neg \bigwedge_i \Box\Diamond A_i$
$\langle 2\rangle 1$. $\sigma \models \varphi_1$
BY $\langle 1\rangle 4$ DEF φ_1
$\langle 2\rangle 2$. $\sigma \models \varphi_2$
$\langle 3\rangle 1$. $\sigma \models \bigvee_i \Diamond\Box\neg A_i$
BY $\langle 1\rangle 4$
$\langle 3\rangle 2$. QED
BY $\langle 3\rangle 1$ DEF φ_2
$\langle 2\rangle 3$. QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$
$\langle 1\rangle 5$. QED
BY $\langle 1\rangle 3$, $\langle 1\rangle 4$

Proposition 4 PROVE

$$\begin{array}{lll} \text{LET } \varphi_1 & \triangleq & \Box(a \Rightarrow \Diamond b) \\ \varphi_2 & \triangleq & \exists\!\!| q : \land\ q = \text{TRUE} \\ & & \qquad \land\ \Box\big(q' \equiv (b \lor (q \land \neg a))\big) \\ & & \qquad \land\ \Box\Diamond q \\ \text{IN} & \varphi_1 \equiv \varphi_2 & \end{array}$$

$\langle 1\rangle 1$. SUFFICES
ASSUME NEW σ, $IsABehavior(\sigma)$
PROVE $\sigma \models \varphi_1 \equiv \varphi_2$
$\langle 1\rangle 2$. ASSUME $\sigma \models \varphi_1$
PROVE $\sigma \models \varphi_2$
The variable q is history-determined in $Hist \triangleq \exists\!\!| q : (q = \text{TRUE}) \land \Box(q' = b \lor (\neg a \land q))$. It remains to show that φ_1 and $Hist$ imply $\Box\Diamond q$. The case $\Box\Diamond a$ implies $\Box\Diamond b$, so $\Box\Diamond q'$. The case $\Diamond\Box\neg a$ is split as $(\Box\neg a) \lor \Diamond(a \land \Box\neg a')$. For the subcase $\Box\neg a$, q starts and remains TRUE. For the subcase $\Diamond(a \land \Box\neg a')$, some infinite suffix of σ has $\neg a$ from the second state onwards, and $\Diamond b$, so $\Diamond q'$. Thus, $\Diamond\Box q'$.
$\langle 1\rangle 3$. ASSUME $\sigma \models \varphi_2$
PROVE $\sigma \models \varphi_1$
The case $(a \land b)$ implies $a \Rightarrow \Diamond b$. The case $(a \land \neg b)$ implies $\neg q'$. By $\Box\Diamond q$, eventually there is a $(q' \land \neg q)$-step. Such a step implies b. The two cases are exhaustive, thus $\Box(a \Rightarrow \Diamond b)$.
$\langle 1\rangle 4$. QED
BY $\langle 1\rangle 2$, $\langle 1\rangle 3$

Proposition 5 PROVE

$$\big(\Box((a \land \textstyle\bigwedge_j \Box\Diamond b_j) \Rightarrow \Diamond c)\big) \equiv \big((\textstyle\bigwedge_j \Box\Diamond b_j) \Rightarrow \Box(a \Rightarrow \Diamond c)\big)$$

$\langle 1\rangle 1$. $\big((a \land \bigwedge_j \Box\Diamond b_j) \Rightarrow \Diamond c\big) \equiv \big((\bigwedge_j \Box\Diamond b_j) \Rightarrow (a \Rightarrow \Diamond c)\big)$
$\langle 1\rangle 2$. QED
BY $\langle 1\rangle 1$, Proposition 3 with $A_i \leftarrow b_j$, $i \leftarrow j$, $B \leftarrow (a \Rightarrow \Diamond c)$

Proposition 6 PROVE

$$\big((\textstyle\bigwedge_j \Box\Diamond b_j) \Rightarrow \Box(a \Rightarrow \Diamond c)\big) \equiv \exists\!\!| q : \big(\textstyle\bigwedge_j \Box\Diamond b_j\big) \Rightarrow \land\ q = \text{TRUE} \\ \land\ \Box(q' = c \lor (q \land \neg a)) \\ \land\ \Box\Diamond q$$

PROOF BY Proposition 4, rules for $\exists\!\!|$.

From this point on we assume that history-determined variables (q, r, etc.) do not occur implicitly (so c, a, etc. below are independent of those history variables), only explicitly where shown.

Proposition 7 DEFINE

$$\begin{aligned}
\varphi_1 &\triangleq \exists\!\!\exists q \;:\; (\textstyle\bigwedge_j \Box\Diamond b_j) \Rightarrow \;\wedge\; q = \text{TRUE} \\
&\qquad\qquad\qquad\qquad\qquad\quad \wedge\; \Box(q' = c \vee (\neg a \wedge q)) \\
&\qquad\qquad\qquad\qquad\qquad\quad \wedge\; \Box\Diamond q \\
\varphi_2 &\triangleq \exists\!\!\exists r, q \;:\; \wedge\; (\textstyle\bigwedge_j \Box\Diamond b_j) \Rightarrow \;\wedge\; q = \text{TRUE} \\
&\qquad\qquad\qquad\qquad\qquad\quad \wedge\; \Box(q' = c \vee (q \wedge \neg a)) \\
&\qquad\qquad\qquad\qquad\qquad\quad \wedge\; \Box\Diamond q \\
&\qquad\qquad\quad \wedge\; r \equiv \text{TRUE} \\
&\qquad\qquad\quad \wedge\; \Box(r' = c \vee (r \wedge \neg a))
\end{aligned}$$

PROVE $\varphi_1 \equiv \varphi_2$

PROOF BY the rules for introducing bound variables, r does not occur in any of the expressions a, c, b_j, q. So r is a history-determined variable.

Proposition 8 DEFINE

$$\begin{aligned}
\varphi_1 &\triangleq \exists\!\!\exists r, q \;:\; \wedge\; (\textstyle\bigwedge_j \Box\Diamond b_j) \Rightarrow \;\wedge\; q = \text{TRUE} \\
&\qquad\qquad\qquad\qquad\qquad\quad \wedge\; \Box(q' = c \vee (\neg a \wedge q)) \\
&\qquad\qquad\qquad\qquad\qquad\quad \wedge\; \Box\Diamond q \\
&\qquad\qquad\quad \wedge\; r = \text{TRUE} \\
&\qquad\qquad\quad \wedge\; \Box(r' = c \vee (\neg a \wedge r)) \\
\varphi_2 &\triangleq \exists\!\!\exists r \;:\; \wedge\; (\textstyle\bigwedge_j \Box\Diamond b_j) \Rightarrow \Box\Diamond r \\
&\qquad\qquad\quad \wedge\; r = \text{TRUE} \\
&\qquad\qquad\quad \wedge\; \Box(r' = c \vee (\neg a \wedge r))
\end{aligned}$$

PROVE $\varphi_1 \equiv \varphi_2$

$\langle 1\rangle 1$. $\varphi_1 \Rightarrow \varphi_2$
Within the consequent, q and r are both history-determined by the same formulas. Thus, $\Box(q = r)$, which together with $\Box\Diamond q$ implies $\Box\Diamond r$ in the consequent. We then eliminate q (recall the assumption that q, r do not occur in a, c, b_j).

$\langle 1\rangle 2$. $\varphi_2 \Rightarrow \varphi_1$
Introduce a history-determined variable r in the consequent. Again, identical formulas imply that $\Box(r = q)$ within the consequent, so $\Box\Diamond q$ implies $\Box\Diamond r$. Omit the conjunct $\Box\Diamond q$.

$\langle 1\rangle 3$. QED
BY $\langle 1\rangle 1$, $\langle 1\rangle 2$

Proposition 9 PROVE

$$\Big(\Box\big((a \wedge \textstyle\bigwedge_j \Box\Diamond b_j) \Rightarrow \Diamond c\big)\Big) \equiv \exists\!\!\exists q \;:\; \begin{array}{l} \wedge\; q = \text{TRUE} \\ \wedge\; \Box(q' = c \vee (\neg a \wedge q)) \\ \wedge\; (\textstyle\bigwedge_j \Box\Diamond b_j) \Rightarrow \Box\Diamond q \end{array} \tag{1}$$

BY Proposition 5, Proposition 6, Proposition 7, Proposition 8.

Proposition 10 ASSUME *For all $m \in 0..d$, for any j with $j \in 0..d \land j \neq m$, variable q_m does not occur in any of P_m, η_{kl}, Q_m.*

PROVE

$$\begin{array}{lll} \text{LET } \varphi_1 & \triangleq & \bigwedge_{m\in 0..d} \Box((P_m \land \big(\bigwedge_{k\in m..d} \bigwedge_{l\in 0..H_k} \Box\Diamond\neg\eta_{kl}\big)) \Rightarrow \Diamond Q_m) \\ \varphi_2 & \triangleq & \exists\!\!\exists q_0, \ldots, q_d : \bigwedge_{m\in 0..d} \land\ q_m \equiv \text{TRUE} \\ & & \qquad\qquad \land\ \Box\big(q'_m = Q_m \lor (\neg P_m \land q_m)\big) \\ & & \qquad\qquad \land\ \big(\bigwedge_{k\in m..d} \bigwedge_{l\in 0..H_k} \Box\Diamond\neg\eta_{kl}\big) \Rightarrow \Box\Diamond q_m \end{array}$$

IN $\varphi_1 \equiv \varphi_2$

$\langle 1\rangle 1$. ASSUME NEW $m \in 0..d$
PROVE $\Box((P_m \land \big(\bigwedge_{k\in m..d} \bigwedge_{l\in 0..H_k} \Box\Diamond\neg\eta_{kl}\big)) \Rightarrow \Diamond Q_m)$
$\equiv \exists\!\!\exists q_m : \land\ q_m$
$\qquad \land\ \Box(q'_m = Q_m \lor (\neg P_m \land q_m))$
$\qquad \land\ \big(\bigwedge_{k\in m..d} \bigwedge_{l\in 0..H_k} \Box\Diamond\neg\eta_{kl}\big) \Rightarrow \Box\Diamond q_m$
PROOF Substitute $a \leftarrow P_m, b_j \leftarrow \neg\eta_{kl}, c \leftarrow Q_m, q \leftarrow q_m$ in Proposition 9.

$\langle 1\rangle 2$. QED
By hypothesis, $\langle 1\rangle 1$,

$$\begin{array}{rl} \bigwedge_{m=0}^{d} \Box((P_m \land \big(\bigwedge_{k\in m..d} \bigwedge_{l\in 0..H_k} \Box\Diamond\neg\eta_{kl}\big)) \Rightarrow \Diamond Q_m) \equiv & \\ \bigwedge_{m=0}^{d} \exists\!\!\exists q_m : \land\ q_m \equiv \text{TRUE} & \equiv \\ \qquad \land\ \Box(q'_m = Q_m \lor (\neg P_m \land q_m)) & \\ \qquad \land\ \big(\bigwedge_{k\in m..d} \bigwedge_{l\in 0..H_k} \Box\Diamond\neg\eta_{kl}\big) \Rightarrow \Box\Diamond q_m & \\ \exists\!\!\exists q_0, \ldots, q_d : \bigwedge_{m=0}^{d} \land\ q_m \equiv \text{TRUE} & \\ \qquad \land\ \Box(q'_m = Q_m \lor (\neg P_m \land q_m)) & \\ \qquad \land\ \big(\bigwedge_{k\in m..d} \bigwedge_{l\in 0..H_k} \Box\Diamond\neg\eta_{kl}\big) \Rightarrow \Box\Diamond q_m & \end{array} \tag{2}$$

Proposition 11 PROVE

$$\begin{array}{lll} \text{LET } \varphi_1 & \triangleq & \bigwedge_{m\in 0..d} \land\ q_m = \text{TRUE} \\ & & \qquad \land\ \Box\big(q'_m = Q_m \lor (\neg P_m \land q_m)\big) \\ & & \qquad \land\ \big(\bigwedge_{k\in m..d} \bigwedge_{l\in 0..H_k} \Box\Diamond\neg\eta_{kl}\big) \Rightarrow \Box\Diamond q_m \\ \varphi_2 & \triangleq & \bigwedge_{m\in 0..d} \land\ q_m = \text{TRUE} \\ & & \qquad \land\ \Box\big(q'_m = Q_m \lor (\neg P_m \land q_m)\big) \\ & & \qquad \land\ \big(\bigwedge_{k\in 0..d} \bigwedge_{l\in 0..H_k} \Box\Diamond\neg\eta_{kl}\big) \Rightarrow \Box\Diamond q_m \end{array}$$

IN $\varphi_1 \equiv \varphi_2$

$\langle 1\rangle 1$. DEFINE $\varphi_1 \triangleq \bigwedge_{m\in 0..d} \land\ q_m = \text{TRUE}$
$\qquad \land\ \Box\big(q'_m = Q_m \lor (\neg P_m \land q_m)\big)$
$\qquad \land\ \big(\bigwedge_{k\in m..d} \bigwedge_{l\in 0..H_k} \Box\Diamond\neg\eta_{kl}\big) \Rightarrow \Box\Diamond q_m$
$\varphi_2 \triangleq \bigwedge_{m\in 0..d} \land\ q_m = \text{TRUE}$
$\qquad \land\ \Box\big(q'_m = Q_m \lor (\neg P_m \land q_m)\big)$
$\qquad \land\ \big(\bigwedge_{k\in 0..d} \bigwedge_{l\in 0..H_k} \Box\Diamond\neg\eta_{kl}\big) \Rightarrow \Box\Diamond q_m$

$\langle 1\rangle 2$. SUFFICES
ASSUME NEW $\sigma, IsABehavior(\sigma)$
PROVE $\sigma \models \varphi_1 \equiv \varphi_2$

⟨1⟩3. ASSUME $\sigma \models \varphi_1$
PROVE $\sigma \models \varphi_2$
OBVIOUS
⟨1⟩4. ASSUME $\sigma \models \varphi_2$
PROVE $\sigma \models \varphi_1$
⟨2⟩1. $\forall k \in 0..d : \forall l \in 0..H_k : \eta_{kl} \Rightarrow (P_k \wedge \neg Q_k) \Rightarrow P_k$
⟨2⟩2. $\forall k \in 0..(d-1) : P_k \Rightarrow Q_{k+1}$
⟨2⟩3. $\forall k \in 0..(d-1) : \forall l \in 0..H_k : \eta_k \Rightarrow P_k \Rightarrow Q_{k+1}$
BY ⟨2⟩1, ⟨2⟩2
⟨2⟩4. $\forall k \in 0..(d-1) : \forall r \in k..d : Q_k \Rightarrow Q_r$
⟨3⟩1. $\forall k \in 0..(d-1) : Q_k \Rightarrow Q_{k+1}$
⟨4⟩1. $\forall k \in 0..(d-1) : P_k \Rightarrow Q_{k+1}$
BY *ChainCondition*
⟨4⟩2. $\forall k \in 0..d : Q_k \Rightarrow P_k$
⟨4⟩3. QED
BY ⟨4⟩1, ⟨4⟩2
⟨3⟩2. $\forall k \in 0..(d-1) : \forall r \in (k+1)..d : Q_k \Rightarrow Q_r$
⟨4⟩1. $\forall r \in (k+1)..d : k < k+1 \leq r \leq d \Rightarrow k < r \leq d$
⟨4⟩2. QED
BY ⟨4⟩1, ⟨3⟩1, *NatInduction*
⟨3⟩3. $\forall k : Q_k \Rightarrow Q_k$
⟨3⟩4. QED
BY ⟨3⟩2, ⟨3⟩3.
⟨2⟩5. $\forall m \in 0..d : \forall k \in 0..(m-1) : \forall l \in 0..H_k : \eta_{kl} \Rightarrow Q_m$
⟨3⟩1. $\forall m \in 0..d : \forall k \in 0..(m-1) : \forall l \in 0..H_k : \eta_{kl} \Rightarrow Q_{k+1}$
⟨4⟩1. $\forall m \in 0..d : \forall k \in 0..(m-1) : k \in 0..(m-1) = 0..(d-1)$
⟨4⟩2. QED
BY ⟨4⟩1, ⟨2⟩3.
⟨3⟩2. $\forall m \in 0..d : \forall k \in 0..(m-1) : Q_{k+1} \Rightarrow Q_m$
⟨4⟩1. $\forall m \in 0..d : \forall k \in 0..(m-1) : m \in (k+1)..d$
⟨5⟩1. $k \in 0..(m-1) \Rightarrow k \leq m-1 \Rightarrow k+1 \leq m$
⟨5⟩2. $m \in 0..d \Rightarrow m \leq d$
⟨5⟩3. QED
BY ⟨5⟩1, ⟨5⟩2.
⟨4⟩2. $\forall m \in 0..d : \forall k \in 0..(m-1) : (k+1) \in 0..(m-1+1) = 0..m \subseteq 0..d$ (the $k+1$ here is k in ⟨2⟩4).
⟨4⟩3. QED
BY ⟨4⟩1, ⟨4⟩2, ⟨2⟩4.
⟨3⟩3. QED
BY ⟨3⟩1, ⟨3⟩2, $\forall m \in 0..d : \forall k \in 0..(m-1) : \forall l \in 0..H_k : \big((\eta_{kl} \Rightarrow Q_{k+1}) \wedge (Q_{k+1} \Rightarrow Q_m)\big) \Rightarrow \eta_{kl} \Rightarrow Q_m$
⟨2⟩6. $\forall m \in 0..d : \forall k \in 0..(m-1) : \forall l \in 0..H_k : \Diamond\Box\eta_{kl} \Rightarrow \Box\Diamond Q_m$
⟨3⟩1. $(A \Rightarrow B) \Rightarrow (\Diamond\Box A \Rightarrow \Diamond\Box B)$
⟨3⟩2. $(\Diamond\Box B) \Rightarrow (\Box\Diamond B)$
⟨3⟩3. $(A \Rightarrow B) \Rightarrow (\Diamond\Box A \Rightarrow \Box\Diamond B)$
BY ⟨3⟩1, ⟨3⟩2.
⟨3⟩4. $(\eta_{kl} \Rightarrow Q_m) \Rightarrow (\Diamond\Box\eta_{kl} \Rightarrow \Box\Diamond Q_m)$
BY ⟨3⟩3 with $A \leftarrow \eta_{kl}$, $B \leftarrow Q_m$

⟨3⟩5. QED
BY ⟨2⟩5, ⟨3⟩4.
⟨2⟩7. $\sigma \models \varphi_2 \Rightarrow \bigwedge_{m \in 0..d} \Box\big(q'_m = Q_m \vee (\neg P_m \wedge q_m)\big)$
⟨2⟩8. $\forall m \in 0..d : \sigma \models \Box\Diamond Q_m \equiv \Box\Diamond q_m$
⟨3⟩1. $\sigma \models \Box\Diamond Q_m \equiv \Box\Diamond q'_m$
BY ⟨2⟩7.
⟨3⟩2. QED
BY ⟨3⟩1 and $\Box\Diamond q'_m \equiv \Box\Diamond q_m$
⟨2⟩9. $\forall m \in 0..d : \forall k \in 0..(m-1) : \forall l \in 0..H_k : \sigma \models \Diamond\Box\eta_{kl} \Rightarrow \Box\Diamond q_m$
BY ⟨2⟩6, ⟨2⟩8
⟨2⟩10. $\forall m \in 0..d : \sigma \models \big(\bigvee_{k \in 0..(m-1)} \bigvee_{l \in 0..H_k} \Diamond\Box\eta_{kl}\big) \Rightarrow \Box\Diamond q_m$
⟨3⟩1. $\forall m \in 0..d : \sigma \models \big(\bigvee_{k \in 0..(m-1)} \bigvee_{l \in 0..H_k} \Diamond\Box\eta_{kl}\big) \Rightarrow \bigvee_{k \in 0..(m-1)} \bigvee_{l \in 0..H_k} \Box\Diamond q_m$
BY ⟨2⟩9
⟨3⟩2. $\forall m \in 0..d : \big(\bigvee_{k \in 0..(m-1)} \bigvee_{l \in 0..H_k} \Box\Diamond q_m\big) \equiv \Box\Diamond q_m$
⟨3⟩3. QED
BY ⟨3⟩1, ⟨3⟩2
⟨2⟩11. QED
BY ⟨2⟩10, as follows:

$$
\begin{aligned}
\sigma \models \varphi_2 \equiv \sigma \models\ & \wedge \textstyle\bigwedge_{m \in 0..d} q = \text{TRUE} \\
& \wedge \textstyle\bigwedge_{m \in 0..d} \Box(q'_m = Q_m \vee (\neg P_m \wedge q_m)) \\
& \wedge \textstyle\bigvee_{k \in 0..d} \bigvee_{l \in 0..H_k} \Diamond\Box\eta_{kl} \vee \Box\Diamond q_m \\
\equiv \sigma \models\ & \wedge \textstyle\bigwedge_{m \in 0..d} q = \text{TRUE} \\
& \wedge \textstyle\bigwedge_{m \in 0..d} \Box(q'_m = Q_m \vee (\neg P_m \wedge q_m)) \\
& \wedge \vee \textstyle\bigvee_{k \in m..d} \bigvee_{l \in 0..H_k} \Diamond\Box\eta_{kl} \\
& \quad \vee \textstyle\bigvee_{k \in 0..(m-1)} \bigvee_{l \in 0..H_k} \Diamond\Box\eta_{kl} \\
& \quad \vee \Box\Diamond q_m \\
\Rightarrow \sigma \models\ & \wedge \textstyle\bigwedge_{m \in 0..d} q = \text{TRUE} \\
& \wedge \textstyle\bigwedge_{m \in 0..d} \Box(q'_m = Q_m \vee (\neg P_m \wedge q_m)) \\
& \wedge \vee \textstyle\bigvee_{k \in m..d} \bigvee_{l \in 0..H_k} \Diamond\Box\eta_{kl} \\
& \quad \vee \Box\Diamond q_m \\
& \quad \vee \Box\Diamond q_m \\
\equiv \sigma \models\ & \wedge \textstyle\bigwedge_{m \in 0..d} q = \text{TRUE} \\
& \wedge \textstyle\bigwedge_{m \in 0..d} \Box(q'_m = Q_m \vee (\neg P_m \wedge q_m)) \\
& \wedge \vee \textstyle\bigvee_{k \in m..d} \bigvee_{l \in 0..H_k} \Diamond\Box\eta_{kl} \\
& \quad \vee \Box\Diamond q_m \\
\equiv \sigma \models\ & \varphi_1
\end{aligned}
$$

⟨1⟩5. QED
BY ⟨1⟩3, ⟨1⟩4

Proposition 12

$$
\begin{aligned}
\text{LET } \varphi_1 \triangleq\ & \textstyle\bigwedge_{m \in 0..d} \Box \vee \neg P_m \\
& \quad \vee \neg \textstyle\bigwedge_{k \in m..d} \bigwedge_{l \in 0..H_k} \Box\Diamond\neg\eta_{kl} \\
& \quad \vee \Diamond Q_m \\
\varphi_2 \triangleq\ & \exists\, q_0, \ldots, q_d : \wedge \textstyle\bigwedge_{m \in 0..d} q_m \equiv \text{TRUE} \\
& \quad \wedge \textstyle\bigwedge_{m \in 0..d} \Box\big(q'_m \equiv Q_m \vee (\neg P_m \wedge q_m)\big) \\
& \quad \wedge \big(\textstyle\bigwedge_{m \in 0..d} \bigwedge_{l \in 0..H_m} \Box\Diamond\neg\eta_{ml}\big) \Rightarrow \textstyle\bigwedge_{m \in 0..d} \Box\Diamond q_m \\
\text{IN}\quad & \varphi_1 \equiv \varphi_2
\end{aligned}
$$

BY Propositions 10 and 11

Proposition 13 ASSUME NEW $m \in 0..d$ PROVE

$$\begin{array}{ll} \text{LET} & \varphi_1 \triangleq \Box\big(Q_m \Rightarrow \bigwedge_{l\in 0..\Xi_m} \Box\Diamond\neg\xi_{ml}\big) \\ & \varphi_2 \triangleq \bigwedge_{l\in 0..\Xi_m} \Box\Diamond\neg\xi_{ml} \\ \text{IN} & \varphi_1 \equiv \varphi_2 \end{array}$$

$\langle 1\rangle 1$. DEFINE $\varphi_1 \triangleq \Box\big(Q_m \Rightarrow \bigwedge_{l\in 0..\Xi_m} \Box\Diamond\neg\xi_{ml}\big)$
$\varphi_2 \triangleq \bigwedge_{l\in 0..\Xi_m} \Box\Diamond\neg\xi_{ml}$
$\langle 1\rangle 2$. SUFFICES
ASSUME NEW $\sigma, IsABehavior(\sigma)$
PROVE $\sigma \models \varphi_1 \equiv \varphi_2$
$\langle 1\rangle 3$. ASSUME $\sigma \models \varphi_2$
PROVE $\sigma \models \varphi_1$
$\langle 2\rangle 1$. $\bigwedge_{l=0}^{\Xi_m} \Box\Diamond\neg\xi_{ml} \equiv \Box \bigwedge_{l=0}^{\Xi_m} \Box\Diamond\neg\xi_{ml}$
PROOF $\bigwedge_{l=0}^{\Xi_m} \Box\Diamond\neg\xi_{ml} \equiv \bigwedge_{l=0}^{\Xi_m} \Box\Box\Diamond\neg\xi_{ml} \equiv \Box \bigwedge_{l=0}^{\Xi_m} \Box\Diamond\neg\xi_{ml}$
$\langle 2\rangle 2$. $(\Box \bigwedge_{l=0}^{\Xi_m} \Box\Diamond\neg\xi_{ml}) \Rightarrow \Box((\neg Q_m) \vee \bigwedge_{l=0}^{\Xi_m} \Box\Diamond\neg\xi_{ml})$
PROOF $(\bigwedge_{l=0}^{\Xi_m} \Box\Diamond\neg\xi_{ml}) \Rightarrow ((\neg Q_m) \vee \bigwedge_{l=0}^{\Xi_m} \Box\Diamond\neg\xi_{ml})$
$\langle 2\rangle 3$. QED
BY $\langle 1\rangle 3$, $\langle 2\rangle 1$, $\langle 2\rangle 2$
$\langle 1\rangle 4$. ASSUME $\sigma \models \varphi_1$
PROVE $\sigma \models \varphi_2$
$\langle 2\rangle 1$. CASE $\sigma \models \Box\neg Q_m$
$\langle 3\rangle 1$. $\forall l \in 0..\Xi_m : \xi_{ml} \Rightarrow Q_m$
BY *ChainCondition*
$\langle 3\rangle 2$. $\forall l \in 0..\Xi_m : \neg Q_m \Rightarrow \neg\xi_{ml}$
BY $\langle 3\rangle 1$
$\langle 3\rangle 3$. $\forall l \in 0..\Xi_m : (\Box\neg Q_m) \Rightarrow (\Box\Diamond\neg\xi_{ml})$
BY $\langle 3\rangle 2$
$\langle 3\rangle 4$. QED
BY $\langle 2\rangle 1$, $\langle 3\rangle 3$
$\langle 2\rangle 2$. CASE $\sigma \models \neg\Box\neg Q_m$
$\langle 3\rangle 1$. $\varphi_1 \wedge \Diamond Q_m \Rightarrow \Diamond \bigwedge_{l\in 0..\Xi_m} \Box\Diamond\neg\xi_{ml}$
$\langle 3\rangle 2$. $\Diamond \bigwedge_{l\in 0..\Xi_m} \Box\Diamond\neg\xi_{ml} \Rightarrow \bigwedge_{l\in 0..\Xi_m} \Diamond\Box\Diamond\neg\xi_{ml} \equiv \bigwedge_{l\in 0..\Xi_m} \Box\Diamond\neg\xi_{ml} \equiv \varphi_2$
BY [4, p.93], $\Diamond(A \wedge B) \Rightarrow (\Diamond A) \wedge (\Diamond B)$.
$\langle 3\rangle 3$. QED
BY $\langle 2\rangle 2$, $\langle 3\rangle 1$, $\langle 3\rangle 2$
$\langle 2\rangle 3$. QED
BY $\langle 1\rangle 4$, $\langle 2\rangle 1$, $\langle 2\rangle 2$
$\langle 1\rangle 5$. QED
BY $\langle 1\rangle 3$, $\langle 1\rangle 4$

Proposition 14 PROVE

$$\begin{array}{ll} \text{LET} & \varphi_1 \triangleq \big(\bigwedge_{m\in 0..d} \bigwedge_{l\in 0..H_m} \Box\Diamond\neg\eta_{ml}\big) \Rightarrow \bigwedge_{m\in 0..d} \bigwedge_{l\in 0..\Xi_m} \Box\Diamond\neg\xi_{ml} \\ & \varphi_2 \triangleq \bigwedge_{m\in 0..d} \bigwedge_{l\in 0..\Xi_m} \Box\Diamond\neg\xi_{ml} \\ \text{IN} & \varphi_1 \equiv \varphi_2 \end{array}$$

⟨1⟩1. DEFINE $\varphi_1 \triangleq \left(\bigwedge_{m\in 0..d} \bigwedge_{l\in 0..H_m} \Box\Diamond\neg\eta_{ml}\right) \Rightarrow \bigwedge_{m\in 0..d} \bigwedge_{l\in 0..\Xi_m} \Box\Diamond\neg\xi_{ml}$
$\varphi_2 \triangleq \bigwedge_{m\in 0..d} \bigwedge_{l\in 0..\Xi_m} \Box\Diamond\neg\xi_{ml}$
⟨1⟩2. SUFFICES
ASSUME NEW $\sigma, IsABehavior(\sigma)$
PROVE $\sigma \models \varphi_1 \equiv \varphi_2$
⟨1⟩3. $\sigma \models \varphi_2 \Rightarrow \varphi_1$
OBVIOUS
⟨1⟩4. $\sigma \models \varphi_1 \Rightarrow \varphi_2$
⟨2⟩1. DEFINE $F \triangleq \bigwedge_{m\in 0..d} \bigwedge_{l\in 0..H_m} \Box\Diamond\neg\eta_{ml}$
⟨2⟩2. CASE $\sigma \models F$
BY ⟨2⟩2 DEF F, φ_1, φ_2
⟨2⟩3. CASE $\sigma \models \neg F$
⟨3⟩1. $(\neg F) \equiv \bigvee_{m\in 0..d} \bigvee_{l\in 0..H_m} \Diamond\Box\eta_{ml}$
⟨3⟩2. $\bigvee_{m\in 0..d} \bigvee_{l\in 0..H_m} \Diamond\Box\eta_{ml} \Rightarrow \exists m \in 0..d : \exists l \in 0..H_m : \Diamond\Box\eta_{ml}$
⟨3⟩3. $\forall m \in 0..d : \forall l \in 0..H_m : \eta_{ml} \Rightarrow \forall k \in 0..d : \forall r \in 0..H_k : \neg\xi_{kr}$
⟨4⟩1. $\forall m \in 0..d : \forall l \in 0..H_m : \eta_{ml} \Rightarrow P_m \wedge \neg Q_m$
⟨4⟩2. $\forall m \in 0..(d-1) : P_m \Rightarrow P_{m+1}$
⟨4⟩3. $\forall m \in 0..(d-1) : \forall q \in (m+1)..d : P_m \Rightarrow P_q$
BY ⟨4⟩2, *NatInduction*
⟨4⟩4. $\forall m \in 0..(d-1) : \forall q \in (m+1)..d : \neg P_q \Rightarrow \neg P_m$
⟨4⟩5. $\forall m \in 0..d : \forall l \in 0..\Xi_m : \xi_{ml} \Rightarrow Q_m$
BY *ChainCondition*
⟨4⟩6. $\forall m \in 1..d : \forall l \in 0..\Xi_m : \xi_{ml} \Rightarrow \neg P_{m-1}$
BY *ChainCondition*
⟨4⟩7. $\xi_{ml} \Rightarrow \neg P_{m-1} \Rightarrow \neg P_{m-2} \Rightarrow \cdots \Rightarrow \neg P_0$
$\forall r \in 0..(m-1) : \forall l \in 0..\Xi_m : \xi_{ml} \Rightarrow \neg P_r$ and $\forall m \in (r+1)..d : \forall l \in 0..\Xi_m : P_r \Rightarrow \neg\xi_{ml}$
⟨4⟩8. $\forall m \in 0..(d-1) : Q_m \Rightarrow Q_{m+1}$
⟨4⟩9. $\forall m \in 0..(d-1) : \forall q \in m..d : \neg Q_q \Rightarrow \neg Q_m$ and $\neg Q_q \Rightarrow \neg Q_q$
⟨4⟩10. $\forall m \in 0..d : \forall l \in 0..\Xi_{ml} : \xi_{ml} \Rightarrow Q_m$
PROOF $\forall m \in 0..d : \forall l \in 0..\Xi_m : \neg Q_m \Rightarrow \neg\xi_{ml}$
⟨4⟩11. $\forall m \in 0..q : \forall l \in 0..\Xi_m : \neg Q_q \Rightarrow (\neg Q_m) \Rightarrow \neg\xi_{ml}$
⟨4⟩12. QED
PROOF $\forall m \in 0..d : \forall l \in 0..H_m : \eta_{ml} \Rightarrow \neg Q_m \Rightarrow \forall k \in 0..m : \forall\theta \in 0..\Xi_k : \neg\xi_{k\theta}$ by ⟨4⟩1, ⟨4⟩11. Also, $\forall m \in 0..d : \forall l \in 0..H_m : \eta_{ml} \Rightarrow P_m \Rightarrow \forall k \in (m+1)..d : \forall\theta \in 0..\Xi_k : \neg\xi_{k\theta}$ by ⟨4⟩7. These imply that $\forall k \in 0..d : \forall\theta \in 0..\Xi_k : \neg\xi_{k\theta}$.
⟨3⟩4. $\forall m \in 0..d : \forall l \in 0..H_m : \Diamond\Box\eta_{ml} \Rightarrow \forall k \in 0..d : \forall r \in 0..\Xi_k : \Diamond\Box\neg\xi_{kr}$
BY ⟨3⟩3
⟨3⟩5. $\forall m \in 0..d : \forall l \in 0..H_m : \Diamond\Box\eta_{ml} \Rightarrow \forall k \in 0..d : \forall r \in 0..\Xi_k : \Box\Diamond\neg\xi_{kr}$
BY ⟨3⟩4, $(\Diamond\Box A) \Rightarrow (\Box\Diamond A)$
⟨3⟩6. $\forall m \in 0..d : \forall l \in 0..H_m : \Diamond\Box\eta_{ml} \Rightarrow \bigwedge_{k\in 0..d} \bigwedge_{r\in 0..\Xi_k} \Box\Diamond\neg\xi_{kr}$
⟨3⟩7. $\bigvee_{m\in 0..d} \bigvee_{l\in 0..H_m} \Diamond\Box\eta_{ml} \Rightarrow \bigwedge_{k\in 0..d} \bigwedge_{r\in 0..\Xi_k} \Box\Diamond\neg\xi_{kr}$
BY ⟨3⟩2, ⟨3⟩6
⟨3⟩8. QED
BY ⟨2⟩3, ⟨3⟩7 DEF φ_1, φ_2
⟨2⟩4. QED
BY ⟨2⟩2, ⟨2⟩3
⟨1⟩5. QED

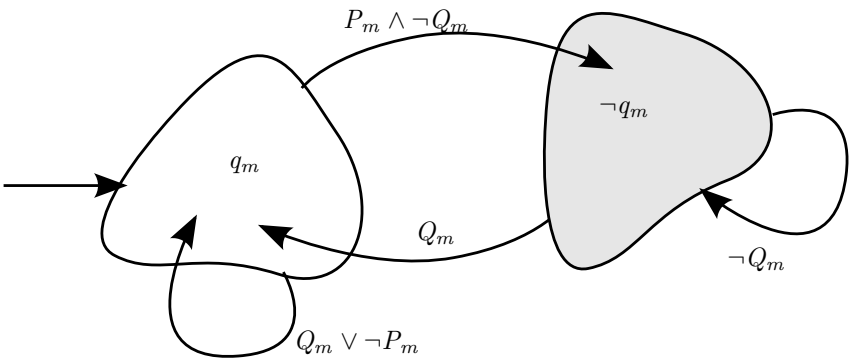

Figure 1: The automaton that corresponds to the auxiliary variable p that reduces memory to $d+1$.

BY $\langle 1 \rangle 3$, $\langle 1 \rangle 4$

Proposition 15 PROVE

$$\begin{array}{l} \Big(\bigwedge_{m \in 0..d} \Box(Q_m \Rightarrow \bigwedge_{l \in 0..\Xi_m} \Box\Diamond\neg\xi_{ml}) \Big) \\ \equiv \vee \ \neg \bigwedge_{m \in 0..d} \bigwedge_{l \in 0..H_m} \Box\Diamond\neg\eta_{ml} \\ \quad \vee \bigwedge_{m \in 0..d} \bigwedge_{l \in 0..\Xi_m} \Box\Diamond\neg\xi_{ml} \end{array}$$

BY Propositions 13 and 14

Lemma 16

$$\begin{array}{lll} \text{LET } \varphi_1 & \triangleq & \Box \bigwedge_{m \in 0..d} \wedge \vee \neg P_m \\ & & \qquad \vee \neg \bigwedge_{k \in m..d} \bigwedge_{l \in 0..H_k} \Box\Diamond\neg\eta_{kl} \\ & & \qquad \vee \Diamond Q_m \\ & & \quad \wedge \ \big(Q_m \Rightarrow \bigwedge_{l \in 0..\Xi_m} \Box\Diamond\neg\xi_{ml}\big) \\ \varphi_2 & \triangleq & \exists q_0, .., q_d \ : \wedge \bigwedge_{m \in 0..d} \wedge \ q_m \equiv \text{TRUE} \\ & & \qquad \wedge \ \Box\big(q'_m \equiv Q_m \vee (\neg P_m \wedge q_m)\big) \\ & & \quad \wedge \vee \neg \bigwedge_{m \in 0..d} \bigwedge_{l \in 0..H_m} \Box\Diamond\neg\eta_{ml} \\ & & \qquad \vee \bigwedge_{m \in 0..d} \wedge \ \Box\Diamond q_m \\ & & \qquad\qquad \wedge \bigwedge_{l \in 0..\Xi_m} \Box\Diamond\neg\xi_{ml} \\ \text{IN} & \varphi_1 \equiv \varphi_2 & \end{array}$$

BY Propositions 12 and 15

Proposition 17 PROVE

$$
\begin{array}{lll}
\text{LET } \varphi_1 & \triangleq & \exists\!\!\mid q_0, .., q_d \ : \ \bigwedge_{m \in 0..d} \land\ q_m = \text{TRUE} \\
& & \qquad\qquad \land\ \Box\big(q'_m = Q_m \lor (\neg P_m \land q_m)\big) \\
& & \qquad\qquad \land\ \Box\Diamond q_m \\
\varphi_2 & \triangleq & \exists\!\!\mid p \ : \ \land\ p = d+1 \\
& & \qquad \land\ \Box p' = \text{CHOOSE}\ \ r \in 0..(d+1) \ : \\
& & \qquad\qquad \land\ \forall m \in 0..d \ : \ (m < r) \Rightarrow \lor\ Q_m \\
& & \qquad\qquad\qquad\qquad\qquad\qquad \lor \land\ \neg P_m \\
& & \qquad\qquad\qquad\qquad\qquad\qquad\quad \land\ p > m \\
& & \qquad\qquad \land\ (r \leq d) \Rightarrow \neg \lor\ Q_r \\
& & \qquad\qquad\qquad\qquad\quad \lor \land\ \neg P_r \\
& & \qquad\qquad\qquad\qquad\qquad \land\ p > r \\
& & \qquad \land\ \Box\Diamond(p = d+1) \\
\text{IN} & \varphi_1 \equiv \varphi_2 &
\end{array}
$$

∃ below is stutter-sensitive temporal quantification.

$$
\begin{array}{l}
Respose(q0,\ \ldots,\ qd) \ \triangleq \\
\quad \forall\, m \in 0\,..\,d : \\
\qquad \land\ qm \equiv \text{TRUE} \\
\qquad \land\ \Box(qm' = Qm \lor (\neg Pm \land qm)) \\
\qquad \land\ \Box\Diamond qm
\end{array}
$$

$$
phi1 \ \triangleq\ \exists\, q0,\ \ldots,\ qd : \ Response(q0,\ \ldots,\ qd)
$$

$$
\begin{array}{l}
ChooseP(r) \ \triangleq \\
\quad \land \quad \forall\, m \in 0\,..\,d : \ (m < r) \Rightarrow \ \lor\ Qm \\
\qquad\qquad\qquad\qquad\qquad\quad \lor \neg Pm \land (p > m) \\
\quad \land \quad (r \leq d) \Rightarrow \neg \lor\ Qr \\
\qquad\qquad\qquad\quad \lor \neg Pr \land (p > r)
\end{array}
$$

$$
\begin{array}{l}
SMP(p) \ \triangleq \\
\qquad \land\ p = d+1 \\
\qquad \land\ \Box(p' = \text{CHOOSE}\ r \in 0\,..\,(d+1) : \ \ ChooseP(r))
\end{array}
$$

$$
\begin{array}{l}
SpecP(p) \ \triangleq \\
\quad \land\ SMP(p) \\
\quad \land\ \Box\Diamond(p = d+1)
\end{array}
$$

$$
phi2 \ \triangleq\ \exists\, p : \ \ SpecP(p)
$$

The satisfaction relation ($\models$) below is of raw TLA+

THEOREM $ReductionWithLinearMemory \ \triangleq$
ASSUME NEW $sigma$, $IsABehavior(sigma)$, $ChainCondition$
PROVE $sigma \models phi1 \equiv phi2$
PROOF
⟨1⟩1. $sigma \models phi1 \Rightarrow phi2$
⟨2⟩1. SUFFICES
ASSUME $sigma \models phi1$

PROVE $sigma \models phi2$

OBVIOUS

$\langle 2 \rangle 2.\ sigma \models \exists\, p :\ SMP(p)$

BY DEF SMP p is history-determined

we will prove liveness of p in $SpecP$

$\langle 2 \rangle 3.$ PICK $tau :\ \land\, IsABehavior(tau)$
$\land\, EqualUpToVars(tau,\ sigma,\ \text{“p”},\ \text{“q0”},\ \ldots,\ \text{“qd”})$
$\land\, tau \models SMP(p) \land Response(q0,\ \ldots,\ qd)$

BY $\langle 2 \rangle 2$

$\langle 2 \rangle 4.$ SUFFICES $tau \models \Box\Diamond(p = d + 1)$

BY $\langle 2 \rangle 3$ DEF $SpecP$, SMP, $phi2$

and that p does not occur in the spec

$\langle 2 \rangle 9.\ tau \models \Box(\exists\, r \in 0 \,..\, (d+1) :\ ChooseP(r))$

$\langle 3 \rangle 1.$CASE $\forall\, m \in 0 \,..\, d :\ Qm \lor (\neg Pm \land (p > m))$

$\langle 4 \rangle 1.\ \forall\, m \in 0 \,..\, d :$
$(m < (d+1)) \Rightarrow (Qm \lor (\neg Pm \land (p > m)))$

BY $\langle 3 \rangle 1$

$\langle 4 \rangle 2.\ \land\, ChooseP(d+1)$
$\land\, (d+1) \in 0 \,..\, (d+1)$

BY $\langle 4 \rangle 1$ DEF $ChooseP$

$\langle 4 \rangle$ QED

BY $\langle 4 \rangle 2$

$\langle 3 \rangle 2.$CASE $\exists\, m \in 0 \,..\, d :\ \neg Qm \land (Pm \lor \neg(p > m))$

$\langle 4 \rangle 1.$ PICK $z \in 0 \,..\, d :$
$\land\ \neg Qz \land (Pz \lor \neg(p > z))$
$\land\ \forall\, t \in 0 \,..\, d :$
$(t < z)\ \Rightarrow\ (Qt \lor (\neg Pt \land (p > t)))$

BY $\langle 3 \rangle 2$, $SmallestNumberPrinciple$

choose the smallest such z.

$\langle 4 \rangle 2.\ (z \leq d) \Rightarrow (\neg Qz \land (Pz \lor \neg(p > z)))$

BY $\langle 4 \rangle 1$

$\langle 4 \rangle 3.\ \land\, ChooseP(z)$
$\land\, z \in 0 \,..\, (d+1)$

BY $\langle 4 \rangle 1$, $\langle 4 \rangle 2$

$\langle 4 \rangle$ QED

BY $\langle 4 \rangle 3$

$\langle 3 \rangle 3.\ \exists\, r \in 0 \,..\, (d+1) :\ ChooseP(r)$

BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$ which are exhaustive

$\langle 3 \rangle$ QED

BY $\langle 3 \rangle 3$

$\langle 2 \rangle 10.\ tau \models \Box \land\, p \in 0 \,..\, (d+1)$
$\land\, ChooseP(p')$

BY $\langle 2 \rangle 3$, $\langle 2 \rangle 9$ DEF SMP

The next step ensures that if ever $p' < (d+1)$, then $\neg qm'$, which starts a chain of $\Diamond Qm$, leading to the bottom, and to $(p = d+1)$ again.

$\langle 2 \rangle 5.\ tau \models \Box \lor\, p' \geq p$
$\lor\, \exists\, m \in 0 \,..\, d :\ \land\, p' = m$
$\land\, \neg qm'$

BY $\langle 2\rangle 10$, $\langle 2\rangle 3$

$\Box(p \in 0..(d+1)$, so if p decreases, then $p' = r \in 0..d$. Since $Choose(p')$, it is $\neg(Qr \lor (\neg Pr \land (p > r))$, thus $\neg qr'$, by DEF *Response*.

$\langle 2\rangle 6.\ \lor\ \neg\ \land\ \Box(qm \in \text{BOOLEAN}\ )$
$\land\ \Box(qm' = Qm \lor (\neg Pm \land qm))$
$\lor\ \Box((\neg qm) \Rightarrow (Qm \equiv qm'))$
BY *PTL*

$\langle 2\rangle 7.\ tau \models\ \land\ \Box((\neg qm \land \neg qm') \Rightarrow \neg Qm)$
$\land\ \Box((\neg qm) \Rightarrow (Qm \equiv qm'))$
$\langle 3\rangle 1.\ tau \models\ \land\ qm = \text{TRUE}$
$\land\ \Box(qm' = Qm \lor (\neg Pm \land qm))$
BY $\langle 2\rangle 1$, $\langle 2\rangle 3$ DEF *EqualUpToVars*, *phi*1
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1$, $\langle 2\rangle 6$

$\langle 2\rangle 8.\ tau \models \forall\, m \in 0\,..\,d :\ \Box((\neg qm) \Rightarrow \Diamond Qm)$
$\langle 3\rangle 1.\ tau \models \forall\, m \in 0\,..\,d :\ \Box\Diamond qm$
BY $\langle 2\rangle 3$ DEF *Response*
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1$, $\langle 2\rangle 7$

$\langle 2\rangle 11.\ tau \models \Box \lor \neg \land (p = m) \land (p \in 0\,..\,d)$
$\land \neg Qm$
$\lor\ p' = m$
$\langle 3\rangle 1.\ \neg Qm \Rightarrow \neg P(m-1) \Rightarrow\ ..\ \Rightarrow \neg P0$
BY *ChainCondition*
$\langle 3\rangle 2.\ (p = m \land p \in 0\,..\,d) \Rightarrow$
$\forall\, r \in 0\,..\,(m-1) :\ (p > r)$
OBVIOUS
$\langle 3\rangle 3.\ (\neg Qm \land (p = m) \land (p \in 0\,..\,d)) \Rightarrow$
$\forall\, r \in 0\,..\,(m-1) :\ \land\ p > r$
$\land \neg Pr$
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$
$\langle 3\rangle 4.\ tau \models \Box($
$(\neg Qm \land (p = m) \land (p \in 0\,..\,d))$
$\Rightarrow (p' \geq m))$
BY $\langle 3\rangle 3$, $\langle 2\rangle 10$ DEF *ChooseP*

Otherwise the second conjunct of *ChooseP* would be violated.

$\langle 3\rangle 5.\ (\neg Qm \land (p = m) \land (p \in 0\,..\,d))$
$\Rightarrow (\neg Qm \land (p \leq m))$
OBVIOUS
$\langle 3\rangle 6.\ tau \models \Box($
$(\neg Qm \land (p = m) \land (p \in 0\,..\,d))$
$\Rightarrow (p' \leq m))$
BY $\langle 3\rangle 5$ DEF *ChooseP* Otherwise $(m < p')$ so it must

be $(Qm \lor (\neg Pm \land (p > m)))$, which is not the case.

$\langle 3\rangle$ QED
BY $\langle 3\rangle 4$, $\langle 3\rangle 6$

$\langle 2\rangle$ DEFINE $TopOrLower(m) \triangleq (0\,..\,(d+1)) \setminus (m\,..\,d)$

⟨2⟩12. $tau \models \Box(Qm \Rightarrow \land\ qm'$
$\land\ p' \in TopOrLower(m)$
⟨3⟩1. $tau \models \Box(Qm \Rightarrow qm')$
BY ⟨2⟩3 DEF *Response*
⟨3⟩2. $Qm \Rightarrow Q(m+1) \Rightarrow\ ..\ \Rightarrow Qd$
BY *ChainCondition*
⟨3⟩3. $tau \models \Box(Qm \Rightarrow (p' \notin m\ ..\ d))$
BY ⟨2⟩10, ⟨3⟩2 DEF *ChooseP* The second conjunct of

ChooseP would be violated by such a p' as r.

⟨3⟩4. $tau \models \Box(p' \in 0\ ..\ (d+1))$
BY ⟨2⟩10, *RawRuleINV*2
⟨3⟩5. $tau \models \Box(Qm \Rightarrow (p' \in ((0\ ..\ (m-1)) \cup \{d+1\})))$
BY ⟨3⟩3, ⟨3⟩4
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩5 DEF *TopOrLower*
⟨2⟩ QED
BY ⟨2⟩5, ⟨2⟩7, ⟨2⟩11, ⟨2⟩12

Initially $p = d+1$ BY DEF *SMP*. Assume $p' < p$. Then BY ⟨2⟩5, $\exists m \in 0..d : (p' = m) \land \neg qm'$. It is $\neg qm' \Rightarrow \neg Qm$. Until qm', it is $(\neg qm \land \neg qm')$. BY ⟨2⟩7 follows that $\neg Qm$ until $\neg qm \land qm'$. BY ⟨2⟩7, $\neg qm \land qm'$ implies Qm. BY ⟨2⟩11, $p' = m = p$ while $\neg Qm$, so while $\neg qm \land \neg qm'$. BY ⟨2⟩12 Qm implies $(p' < p = m) \lor (p' = d+1)$. So $\Box((p' < p) \Rightarrow \Diamond Qm')$ (because we started with $\neg Qm$, and $\Diamond Qm$). So p is strictly decreasing until $p' = d+1$ (by induction over steps of the behavior).

⟨1⟩2. $sigma \models phi2 \Rightarrow phi1$
⟨2⟩1. SUFFICES
ASSUME $sigma \models phi2$
PROVE $sigma \models phi1$
OBVIOUS
⟨2⟩2. $sigma \models \exists\, p :\ SpecP(p)$
BY ⟨2⟩1 DEF *phi*2
⟨2⟩3. $sigma \models \exists\, q0,\ ..\ ,\ qd :\ \forall\, m \in 0\ ..\ d :$
$\land\ qm = \text{TRUE}$
$\land\ \Box(qm' = Qm \lor (\neg Pm \land qm))$
OBVIOUS $q_0, \ldots, q_d$ are history-determined.
⟨2⟩4. PICK $tau :\ \land\ IsABehavior(tau)$
$\land\ EqualUpToVars(tau,\ sigma,\ \text{“p”},\ \text{“q0”},\ ..\ ,\ \text{“qd”})$
$\land\ tau \models\ \land\ SpecP(p)$
$\land\ \forall\, m \in 0\ ..\ d :$
$\land\ qm = \text{TRUE}$
$\land\ \Box(qm' = Qm \lor (\neg Pm \land qm))$
BY ⟨2⟩2, ⟨2⟩3
⟨2⟩5. SUFFICES $tau \models \forall\, m \in 0\ ..\ d :\ \Box\Diamond qm$
BY ⟨2⟩4 DEF *phi*1, *Response*
⟨2⟩6. SUFFICES $tau \models \forall\, m \in 0\ ..\ d :\ \Box((qm \land \neg qm')\ \Rightarrow\ \Diamond qm')$
BY ⟨2⟩4, *PTL* whenever any q_m becomes FALSE,

it eventually becomes again TRUE. Thus, the goal from ⟨2⟩5 follows.

⟨2⟩7. $tau \models \forall\, m \in 0\ ..\ d :\ \Box((qm \land \neg qm')\ \Rightarrow\ (\neg Qm \land Pm))$
BY ⟨2⟩4
⟨2⟩8. $tau \models \forall\, m \in 0\ ..\ d :\ \Box\Diamond(p' > m)$

BY $\langle 2\rangle 4$ DEF *SpecP*

$\langle 2\rangle 9$. $tau \models \forall\, m \in 0\,..\,d :\ \Box((\neg Qm \land Pm) \ \Rightarrow\ (p' \leq m))$

BY $\langle 2\rangle 4$ DEF *SpecP*, *SMP*, *ChooseP*

we proved under $\langle 1\rangle 1$ that $ChooseP(p')$ holds.

$\langle 2\rangle 10$. $tau \models \forall\, m \in 0\,..\,d :\ \Box((p' > m) \Rightarrow (Qm \lor (\neg Pm \land (p > m))))$

BY $\langle 2\rangle 4$ DEF *SpecP*, *SMP*, *ChooseP*

$\langle 2\rangle 11$. $tau \models \forall\, m \in 0\,..\,d :$
$\Box((\neg Qm \land Pm) \ \Rightarrow\ \Diamond((p \leq m) \land (p' > m))$

BY $\langle 2\rangle 9$, $\langle 2\rangle 8$

$\langle 2\rangle 12$. $tau \models \forall\, m \in 0\,..\,d :\ \Box((\neg Qm \land Pm) \ \Rightarrow\ \Diamond Qm)$

BY $\langle 2\rangle 10$, $\langle 2\rangle 11$

$\langle 2\rangle 13$. $tau \models \forall\, m \in 0\,..\,d :\ \Box(Qm \Rightarrow qm')$

BY $\langle 2\rangle 4$

$\langle 2\rangle 14$. $tau \models \forall\, m \in 0\,..\,d :\ \Box((\neg Qm \land Pm) \ \Rightarrow\ \Diamond qm')$

BY $\langle 2\rangle 12$, $\langle 2\rangle 13$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 7$, $\langle 2\rangle 14$

$\langle 1\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle 2$

References

[1] L. Lamport, "How to write a 21st century proof," *Journal of fixed point theory and applications*, vol. 11, no. 1, pp. 43–63, 2012.

[2] M. Abadi and L. Lamport, "An old-fashioned recipe for real time," *TOPLAS*, vol. 16, no. 5, pp. 1543–1571, September 1994.

[3] I. Filippidis and R. M. Murray, "Symbolic construction of GR(1) contracts for systems with full information," in *ACC*, 2016, pp. 782–789.

[4] L. Lamport, *Specifying Systems: The TLA$^+$ language and tools for hardware and software engineers*. Addison-Wesley, 2002.