Class Notes for CS 819A4 - Spring 2003

9. Proving the Hypothetical Frame Rule

John C. Reynolds
Department of Computer Science
Carnegie Mellon University

Revised May 23, 2003

I have not had time to work out a full proof of the hypothetical frame rule. The following discussion is based on preliminary work by Peter O'Hearn ("Notes on the Second-Order Frame Rule"). It limits the HFR to a single hypothesis, and, more seriously, ignores the store. Many parts of the (potential) proof are omitted. But I hope the critical aspects have been covered.

A Simplified Store-Free Model

We use the model developed in the previous section, but limited to the empty set of ordinary variables ($V = \{\}$) and a single command variable ($K = \{k\}$). Thus we have

$$\begin{aligned}
\text{Heaps} &= \bigcup_{A \overset{\text{fin}}{\subseteq} \text{Addresses}} (A \to \text{Values}) \\
\text{States} &= \text{Heaps} \\
\text{Nonterminals} &= \text{Comm} \times \text{States} \\
\text{Terminals} &= \text{States} \cup \{\mathbf{abort}, \bot\} \\
\text{CMeanings} &\subseteq \mathcal{P}(\text{States} \times \text{Terminals}) \\
\text{Environments} &= \{k\} \to \text{CMeanings},
\end{aligned}$$

and when $\eta \in$ Environments,

$$\overset{\eta}{\rightsquigarrow} \in \mathcal{P}(\text{Nonterminals} \times (\text{Nonterminals} \cup \text{Terminals})).$$

The Call Rule

When $h, \tau \in \eta k$:

$$\frac{}{k, h \overset{\eta}{\rightsquigarrow} \tau.}$$

Thus,

$$[\![k]\!]_{\text{comm}}\eta = \eta(k).$$

Command Meanings

Suppose $\rho \subseteq \text{States} \times \text{Terminals}$.

- When $h, \textbf{abort} \notin \rho$, we say that ρ, h is *safe*.
- When $h, \textbf{abort} \notin \rho$ and $h, \perp \notin \rho$, we say that ρ, h *must terminate normally*.

Then $\rho \in \text{CMeanings}$ iff:

- Safety Monotonicity
  - If ρ, h_0 is safe and $h_0 \subseteq h$, then ρ, h is safe.
  - If ρ, h_0 must terminate normally and $h_0 \subseteq h$, then ρ, h must terminate normally.
- The Frame Property
  - Suppose ρ, h_0 is safe, $h_0 \subseteq h$, and $h, h' \in \rho$. Then there is a heap h'_0 such that $h_0, h'_0 \in \rho$ and $h' = h'_0 \cdot (h - h_0)$.

(Here and later, $h = h' \cdot h''$ is meant to imply $h' \perp h''$.)

Since, according to Propositions 7 and 8 in Section 2, the (large-step) meanings of all commands not containing calls satisfy these properties, we expect that, by limiting the meaning of command identifiers to CMeanings, we will insure that the meanings of all commands satisfy these properties.

Note, however, that CMeanings contains relations that are not total. (Thus, "ρ, h must terminate normally" means that neither $h, \textbf{abort}$ nor $h, \perp$ belong to ρ, not that some h, h' belongs to ρ.)

Extending Specifications to Command Meanings

When p and q are assertions and ρ is a command meaning, we write

$$\begin{aligned}
\{p\}\ \rho\ \{q\} \ \text{ iff }\ \forall h \in \text{States}.\ & h \vDash p \text{ implies} \\
& \rho, h \text{ is safe} \\
& \text{and } \big(\forall h' \in \text{States}.\ h, h' \in \rho \text{ implies } h' \vDash q\big), \\
[\,p\,]\ \rho\ [\,q\,] \ \text{ iff }\ \forall h \in \text{States}.\ & h \vDash p \text{ implies} \\
& \rho, h \text{ must terminate normally} \\
& \text{and } \big(\forall h' \in \text{States}.\ h, h' \in \rho \text{ implies } h' \vDash q\big).
\end{aligned}$$

When η is an environment, p and q are assertions, and c is a command, we write

$$\eta \Vdash \{p\}\ c\ \{q\} \ \text{ iff }\ \{p\}\ (\llbracket c \rrbracket_{\text{comm}} \eta)\ \{q\},$$

$$\eta \Vdash [\,p\,]\ c\ [\,q\,] \ \text{ iff }\ [\,p\,]\ (\llbracket c \rrbracket_{\text{comm}} \eta)\ [\,q\,].$$

When p, q, a, and b are assertions, k is a command identifier, and c is a command, we write

$$\begin{aligned}
&(\{p\}\ k\ \{q\} \vdash \{a\}\ c\ \{b\}) \ \text{ iff} \\
&\qquad \forall \eta \in \text{Environments}.\ \eta \Vdash \{p\}\ k\ \{q\} \text{ implies } \eta \Vdash \{a\}\ c\ \{b\}.
\end{aligned}$$

Henceforth, we will only consider partial correctness.

The "Best" Relation

For assertions p and q, we define $\mathrm{best}(p, q)$ to be the command meaning such that

- $h, \mathbf{abort} \in \mathrm{best}(p, q)$ iff $\neg(h \vDash p \ast \mathbf{true})$,
- $h, \perp \in \mathrm{best}(p, q)$ always,
- $h, h' \in \mathrm{best}(p, q)$ iff

  $(h \vDash p \ast \mathbf{true})$ implies

$$\left.\begin{array}{l} \forall h_p.\ h_p \subseteq h \text{ and } h_p \vDash p \\ \qquad \text{implies } \exists h'_q.\ h' = h'_q \cdot (h - h_p) \text{ and } h'_q \vDash q. \end{array}\right\} \tag{1}$$

(Here and later, $h = h' \cdot h''$ is meant to imply $h' \perp h''$.)

Proposition 12 *Condition* (1) *is equivalent to*

$$\forall s.\ (h \vDash p \ast s) \text{ implies } (h' \vDash q \ast s), \tag{2}$$

and to

$$\forall t.\ (h \vDash p \ast (q \mathrel{-\!\!\ast} t)) \text{ implies } (h' \vDash t), \tag{3}$$

and, when q is intuitionistic, to

$$\forall_{\text{intuit}} t.\ (h \vDash p \ast (q \mathrel{-\!\!\ast} t)) \text{ implies } (h' \vDash t). \tag{4}$$

In (2) and (3), the quantified variables s and t are meant to range over all assertions (or equivalently, all states). In (4), t is meant to range over all intuitionistic assertions.

The "Best" Relation (continued)

Proof To show that (1) implies (2), assume (1) and $h \vDash p \; * \; s$. Then there is an $h_p \subseteq h$ such that $h_p \vDash p$ and $h - h_p \vDash s$. Then by (1), there is an h'_q such that h' partitions into $h'_q \cdot (h - h_p)$, and $h'_q \vDash q$. Thus $h' \vDash q \; * \; s$.

To show that (2) implies (1), assume (2), $h_p \subseteq h$, and $h_p \vDash p$. Let s be the assertion that is only true for the state $h - h_p$. Then $h \vDash p \; * \; s$, and by (2), $h' \vDash q \; * \; s$. Thus there is an $h'_q \subseteq h'$ such that $h'_q \vDash q$ and $h' - h'_q \vDash s$. But $h' - h'_q \vDash s$ implies $h' - h'_q = h - h_p$.

To show that (2) implies (3), assume (2) and $h \vDash p \; * \; (q \mathrel{-\!\!*} t)$. Taking s to be $q \mathrel{-\!\!*} t$ in (2) gives $h' \vDash q \; * \; (q \mathrel{-\!\!*} t)$. Then, since $q \; * \; (q \mathrel{-\!\!*} t) \Rightarrow t$, we have $h' \vDash t$.

To show that (3) implies (2), assume (3) and $h \vDash p \; * \; s$. Since $s \Rightarrow (q \mathrel{-\!\!*} (q \; * \; s))$, we have $h \vDash p \; * \; (q \mathrel{-\!\!*} (q \; * \; s))$. Then taking t to be $q \; * \; s$ in (3) gives $h' \vDash q \; * \; s$.

Now assume that q is intuitionistic. The proof of equivalence between (4) and (2) is similar to that for (3) and (2), except that, in the final step where one takes t to be $q \; * \; s$, t is intuitionistic since q is intuitionistic. END OF PROOF

In what follows we will not use Proposition 12. In O'Hearn's original proof, however, (3) and (implicitly) (4) are used instead of (1) in the definition of $\text{best}(p, q)$.

Why $\mathrm{best}(p,q)$ is Best

Proposition 13 *The relation* $\mathrm{best}(p,q)$ *satisfies*

1. $\mathrm{best}(p,q) \in \mathrm{CMeanings}$,
2. $\{p\}\ \mathrm{best}(p,q)\ \{q\}$,
3. $\forall \rho \in \mathrm{Cmeanings}.\ \{p\}\ \rho\ \{q\}$ *implies* $\rho \subseteq \mathrm{best}(p,q)$.

In other words, $\mathrm{best}(p,q)$ is the largest command meaning satisfying the specification $\{p\} - \{q\}$.

PROOF (Part 1) To see that $\mathrm{best}(p,q)$ satisfies safety monotonicity, suppose $\mathrm{best}(p,q), h_0$ is safe and $h_0 \subseteq h$. Then $h_0, \mathbf{abort} \notin \mathrm{best}(p,q)$, so that, by the definition of $\mathrm{best}(p,q)$, $h_0 \vDash p * \mathbf{true}$. Then $h \vDash p * \mathbf{true}$, so that $h, \mathbf{abort} \notin \mathrm{best}(p,q)$, and $\mathrm{best}(p,q), h$ is safe.

Trivially, since $h_0, \perp \in \mathrm{best}(p,q)$ for all h_0, there is no h_0 for which $\mathrm{best}(p,q), h_0$ must terminate normally.

To see that $\mathrm{best}(p,q)$ satisfies the frame property, suppose that $\mathrm{best}(p,q), h_0$ is safe (so that, as above, $h_0 \vDash p * \mathbf{true}$), $h_0 \subseteq h$, and $h, h' \in \mathrm{best}(p,q)$. We must show that there is a heap h_0' such that $h_0, h_0' \in \mathrm{best}(p,q)$ and $h' = h_0' \cdot (h - h_0)$.

First, we show that $h - h_0 \subseteq h'$. Since $h_0 \subseteq h$ and $h_0 \vDash p * \mathbf{true}$, there is an $h_p \subseteq h_0 \subseteq h$ such that $h_p \vDash p$. Then, since $h, h' \in \mathrm{best}(p,q)$, by (1) in the definition of $\mathrm{best}(p,q)$ we find that there is an h_q' such that $h' = h_q' \cdot (h - h_p)$. Thus, since $h_p \subseteq h_0$, we have $h - h_0 \subseteq h - h_p \subseteq h'$.

Thus, we may define $h_0' \stackrel{\mathrm{def}}{=} h' - (h - h_0)$, so that $h' = h_0' \cdot (h - h_0)$.

Finally, to show that $h_0, h'_0 \in \text{best}(p, q)$, suppose h_p is any subset of h_0 such that $h_p \vDash p$. Since $h, h' \in \text{best}(p, q)$ and $h_p \subseteq h$, (1) shows that there is an h'_q such that $h' = h'_q \cdot (h - h_p)$ and $h'_q \vDash q$. Since $h_p \subseteq h_0 \subseteq h$, we have $h' = h'_q \cdot (h - h_0) \cdot (h_0 - h_p)$, and since $h'_0 = h' - (h - h_0)$, we have $h'_0 = h'_q \cdot (h_0 - h_p)$. Thus, by (1), $h_0, h'_0 \in \text{best}(p, q)$.

(Part 2) Suppose $h \vDash p$. Then $h \vDash p \ast \textbf{true}$, so that $h, \textbf{abort} \notin \text{best}(p, q)$, and $\text{best}(p, q), h$ is safe.

In addition, suppose $h, h' \in \text{best}(p, q)$. Since $h \vDash p$, in (1) we can take $h_p = h$. Then $h' = h'_q \cdot (h - h_p)$ and $h'_q \vDash q$ give $h' \vDash q$.

(Part 3) We assume that ρ is a command meaning such that $\{p\}\ \rho\ \{q\}$. Then we must show $\rho \subseteq \text{best}(p, q)$.

If $h, \textbf{abort} \notin \text{best}(p, q)$, then $h \vDash p \ast \textbf{true}$, so that there is an $h_p \subseteq h$ such that $h_p \vDash p$. Then from $\{p\}\ \rho\ \{q\}$ we have that ρ, h_p is safe, and from safety monotonicity we have that ρ, h is safe, i.e., $h, \textbf{abort} \notin \rho$.

$h, \perp \in \text{best}(p, q)$ always holds.

If $h, h' \in \rho$, we can use (1) to show that $h, h' \in \text{best}(p, q)$. For suppose $h_p \subseteq h$ and $h_p \vDash p$. From $\{p\}\ \rho\ \{q\}$ we know that ρ, h_p is safe. Then from the frame property, there is an h'_q such that $h_p, h'_q \in \rho$ and $h' = h'_q \cdot (h - h_p)$. Then from $\{p\}\ \rho\ \{q\}$, we have $h'_q \vDash q$, and (1) gives $h, h' \in \text{best}(p, q)$. END OF PROOF

More Properties of Command Meanings and Specifications

Proposition 14 *Suppose ρ and ρ' are command meanings, η, η', and $\eta_{p,q}$ are environments, and $\eta_{p,q}k = \mathrm{best}(p, q)$. Then*

1. *$\eta k \subseteq \eta' k$ implies $[\![c]\!]_{\mathrm{comm}}\eta \subseteq [\![c]\!]_{\mathrm{comm}}\eta'$.*

2. *$\rho \subseteq \rho'$ implies $(\{p\}\ \rho'\ \{q\}$ implies $\{p\}\ \rho\ \{q\})$.*

3. *$\{p\}\ \rho\ \{q\}$ iff $\rho \subseteq \mathrm{best}(p, q)$.*

4. *$(\{p\}\ k\ \{q\} \vdash \{a\}\ c\ \{b\})$ iff $\eta_{p,q} \Vdash \{a\}\ c\ \{b\}$.*

Proof (1) By induction on the structure of commands.

(2) By the definition of $\{p\}\ \rho\ \{q\}$.

(3) The forward implication follows from Part 3 of Proposition 13. The backward implication follows from Part 2 of the present proposition and Part 2 of Proposition 13.

(4) Suppose $\{p\}\ k\ \{q\} \vdash \{a\}\ c\ \{b\}$. From Part 2 of Proposition 13, we have $\{p\}\ \eta_{p,q}k\ \{q\}$, so that $\eta_{p,q} \Vdash \{p\}\ k\ \{q\}$. Then the definition of $\{p\}\ k\ \{q\} \vdash \{a\}\ c\ \{b\}$ gives $\eta_{p,q} \Vdash \{a\}\ c\ \{b\}$.

On the other hand, suppose $\eta_{p,q} \Vdash \{a\}\ c\ \{b\}$ and $\eta \Vdash \{p\}\ k\ \{q\}$. Then we must show $\eta \Vdash \{a\}\ c\ \{b\}$. But $\eta \Vdash \{p\}\ k\ \{q\}$ implies $\{p\}\ \eta k\ \{q\}$, which implies $\eta k \subseteq \eta_{p,q}k$ by Part 3 of the present proposition. Then Part 1 shows that $[\![c]\!]_{\mathrm{comm}}\eta \subseteq [\![c]\!]_{\mathrm{comm}}\eta_{p,q}$, and Part 2 shows that $\eta_{p,q} \Vdash \{a\}\ c\ \{b\}$ implies $\eta \Vdash \{a\}\ c\ \{b\}$.

END OF PROOF

Environmental Safety and Framing

Henceforth, we fix a particular instance of the hypothetical frame rule (HFR):

$$\frac{\{p\}\ k\ \{q\} \vdash \{a\}\ c\ \{b\}}{\{p * r\}\ k\ \{q * r\} \vdash \{a * r\}\ c\ \{b * r\}.}$$

We also fix η_0 and η_1 to be the environments such that

$$\eta_0 k = \mathrm{best}(p, q) \qquad \eta_1 k = \mathrm{best}(p * r, q * r).$$

Then the following two properties will be sufficient to prove the HFR:

- Environmental Safety If

  1. $[\![c]\!]_{\mathrm{comm}}\eta_0, h_0$ is safe,
  2. $h_r \vDash r$, and
  3. $h = h_0 \cdot h_r$,

  then $[\![c]\!]_{\mathrm{comm}}\eta_1, h$ is safe.

- Environmental Framing If

  1. $[\![c]\!]_{\mathrm{comm}}\eta_0, h_0$ is safe,
  2. $h_r \vDash r$,
  3. $h = h_0 \cdot h_r$, and
  4. $h, h' \in [\![c]\!]_{\mathrm{comm}}\eta_1$,

  then

  $$\exists h'_0, h'_r.\ h' = h'_0 \cdot h'_r \text{ and } h'_r \vDash r \text{ and } h_0, h'_0 \in [\![c]\!]_{\mathrm{comm}}\eta_0.$$

Proving the Hypothetical Frame Rule

Proposition 15 *If Environmental Safety and Environmental Framing hold, then the hypothetical frame rule is sound.*

Proof By Part 4 of Proposition 14, it is sufficient to assume $\eta_0 \Vdash \{a\}\ c\ \{b\}$ and show $\eta_1 \Vdash \{a * r\}\ c\ \{b * r\}$.

Suppose $h \vDash a * r$. Then we can partition h into $h_0 \cdot h_r$ such that $h_0 \vDash a$ and $h_r \vDash r$. Since $\eta_0 \Vdash \{a\}\ c\ \{b\}$, we know that $[\![c]\!]_{\mathrm{comm}}\eta_0, h_0$ is safe, and so $[\![c]\!]_{\mathrm{comm}}\eta_1, h$ is safe by Environmental Safety.

Now suppose further that $h, h' \in [\![c]\!]_{\mathrm{comm}}\eta_1$. By Environmental Framing, we can partition h' into $h'_0 \cdot h'_r$ so that $h'_r \vDash r$ and $h_0, h'_0 \in [\![c]\!]_{\mathrm{comm}}\eta_0$. Then the assumption $\eta_0 \Vdash \{a\}\ c\ \{b\}$ implies that $h'_0 \vDash b$, so that $h' \vDash b * r$. END OF PROOF

Proving Environmental Safety

Proposition 16 *Environmental Safety holds.*

PROOF The proof is by induction on the structure of c. We give only the case where c is k. There we must show that, if

1. $\mathrm{best}(p, q), h_0$ is safe,
2. $h_r \vDash r$, and
3. $h = h_0 \cdot h_r$,

then $\mathrm{best}(p * r, q * r), h$ is safe.

Since $\mathrm{best}(p, q), h_0$ is safe, $h_0, \mathbf{abort} \notin \mathrm{best}(p, q)$, and the definition of best shows that $h_0 \vDash p * \mathbf{true}$. Then $h = h_0 \cdot h_r \vDash p * r * \mathbf{true}$, and the definition of best shows that $\mathrm{best}(p * r, q * r), h$ is safe. END OF PROOF

Some Terminology

Any subset of a heap is a heap. To emphasize this fact, we will often call a subset of a heap h a *subheap of* h.

We call two heaps *compatible* if their union is a heap or, equivalently, if they are both subsets of the same heap.

When $h \vDash p$, we say that h *models* p. When $h \vDash p$ and there is no proper subheap $h' \subset h$ such that $h' \vDash p$, we write $h \vDash_{\min} p$, and say that h is a *minimum model* of p,

We say that p is *precise* if, whenever h_1 and h_2 are compatible models of p, $h_1 = h_2$.

We say that p is *supported* if, whenever h_1 and h_2 are compatible models of p, there is a common subheap h' of h_1 and h_2 that also models p.

Properties of Precise and Supported Assertions

Proposition 17

1. *If* $h \vDash p$*, then there is a subheap* $h_m \subseteq h$ *such that* $h_m \vDash_{\min} p$.

2. *If* $h \vDash p * q$ *and either* p *is precise or* q *is intuitionistic, then there is a subheap* $h_p \subseteq h$ *such that* $h_p \vDash_{\min} p$ *and* $h - h_p \vDash q$.

3. *Suppose* h *and* $h_{\min}$ *are compatible heaps,* $h \vDash p$*, and* $h_{\min} \vDash_{\min} p$*. If* p *is supported then* $h_{\min} \subseteq h$*. If* p *is precise then* $h_{\min} = h$.

4. *Suppose* h *and* h_p *are compatible heaps,* $h \vDash p * q$*, and* $h_p \vDash_{\min} p$*. If* p *is precise, or* p *is supported and* q *is intuitionistic, then* $h - h_p \vDash q$.

5. p *is precise iff* p *is supported and every heap that models* p *is a minimal model of* p.

Proof

1. Form the decreasing sequence $h = h_0 \supset h_1 \supset \cdots \supset h_m$ by taking each h_{i+1} to be a proper subheap of h_i that models p, until one obtains an h_m such that no proper subheap models p. Since the size of the finite domains of the h_i decreases, this sequence must terminate.

2. Since $h \vDash p \ast q$, we know that there is an $h' \subseteq h$ such that $h' \vDash p$ and $h - h' \vDash q$. If p is precise, h' will be a minimal model of p and can be taken to be h_p. Otherwise, there will be an $h_p \subseteq h'$ that will be a minimal model of p, and $h - h_p \supseteq h - h'$. Then if q is intuitionistic, since $h - h' \vDash q$, we have $h - h_p \vDash q$.

3. Suppose p is supported. Then there is an h' that models p and is a common subheap of h and h_{min}. But h' must equal to h_{min} since otherwise it would be a proper subheap of a minimum model of p. Thus $h_{\mathrm{min}} \subseteq h$.

   The case where p is precise is obvious.

4. Since $h \vDash p \ast q$ there is an $h' \subseteq h$ such that $h' \vDash p$ and $h - h' \vDash q$. By Part 3 of this proposition, if p is precise, then $h_p = h'$, so that $h - h_p \vDash q$, while if p is supported, then $h_p \subseteq h'$, so that $h - h_p \supseteq h - h'$, and $h - h_p \vDash q$ holds when q is intuitionistic.

5. Suppose p is supported and its models are all minimal. Let h_1 and h_2 be subheaps of h such that $h_1 \vDash p$ and $h_2 \vDash p$. By Part 3 of this proposition, $h_1 \subseteq h_2$ since h_1 is minimal, and $h_2 \subseteq h_1$ since h_2 is minimal. Thus $h_1 = h_2$.

   The converse is left to the reader.

END OF PROOF

Proving Environmental Framing

Proposition 18 *Environmental Framing holds in each of two cases:*

1. *p is precise, or p is supported and q is intuitionistic,*

2. *r is precise, or r is supported and q is intuitionistic.*

Proof The proof is by induction on the structure of c. We give only the case where c is k. There we must show that, if

1. $\mathrm{best}(p, q), h_0$ is safe,

2. $h_r \vDash r$,

3. $h = h_0 \cdot h_r$, and

4. $h, h' \in \mathrm{best}(p * r, q * r)$,

then

$$\exists h'_0, h'_r.\ h' = h'_0 \cdot h'_r \text{ and } h'_r \vDash r \text{ and } h_0, h'_0 \in \mathrm{best}(p, q).$$

Assume 1 to 4. From 1 and the definition of $\mathrm{best}(p, q)$, we have $h_0 \vDash p * \mathbf{true}$, so that there is some $h_p \vDash p$ such that h_0 can be partitioned into $h_p \cdot (h_0 - h_p)$. In Case 1, by Part 2 of Proposition 17, we can assume $h_p \vDash_{\min} p$.

Moreover, $h = h_0 \cdot h_r = h_p \cdot h_r \cdot (h_0 - h_p) \vDash p * r * \mathbf{true}$, so that, from Assumption 4, and (1) for the definition of $\mathrm{best}(p * r, q * r)$ (taking h_p to be $h_p \cdot h_r$ and renaming h'_q to h'_{qr}), we know that there is an h'_{qr} such that

$$h' = h'_{qr} \cdot (h - h_p \cdot h_r) = h'_{qr} \cdot (h_0 - h_p) \text{ and } h'_{qr} \vDash q * r.$$

Then there are h'_q and h'_r such that $h'_{qr} = h'_q \cdot h'_r$, and $h'_q \vDash q$ and $h'_r \vDash r$. In Case 2, by Part 2 of Proposition 17, we can assume $h'_r \vDash_{\min} r$.

We define $h'_0 \stackrel{\text{def}}{=} h'_q \cdot (h_0 - h_p)$, so that $h' = h'_q \cdot h'_r \cdot (h_0 - h_p) = h'_0 \cdot h'_r$.

Our remaining task is to use (1) to show that $h_0, h'_0 \in \text{best}(p, q)$. Thus we assume that $\tilde{h}_p \subseteq h_0$ and $\tilde{h}_p \vDash p$, and we must show that there is an $\tilde{h}'_q$ such that $h'_0 = \tilde{h}'_q \cdot (h_0 - \tilde{h}_p)$ and $\tilde{h}'_q \vDash q$. (We have decorated $\tilde{h}_p$ and $\tilde{h}'_q$ to indicate that they may be distinct from the h_p and h'_q occurring earlier in this proof.)

(Case 1) Since $h_p \vDash_{\min} p$, $\tilde{h}_p \vDash p$, and both h_p and $\tilde{h}_p$ are subsets of h_0, by Part 3 of Proposition 17 we have $h_p \subseteq \tilde{h}_p \subseteq h_0$ and, when p is precise, $h_p = \tilde{h}_p$. Thus $h'_0 = h'_q \cdot (h_0 - h_p) = h'_q \cdot (h_0 - \tilde{h}_p) \cdot (\tilde{h}_p - h_p)$, so that we can define $\tilde{h}'_q = h'_q \cdot (\tilde{h}_p - h_p)$ to obtain $h'_0 = \tilde{h}'_q \cdot (h_0 - \tilde{h}_p)$. If p is precise, then $\tilde{h}'_q = h'_q$ insures $\tilde{h}'_q \vDash q$, while if q is intuitionistic, then $\tilde{h}'_q \supseteq h'_q$ is enough to insure $\tilde{h}'_q \vDash q$.

(Case 2) We have $\tilde{h}_p \cdot h_r \subseteq h_0 \cdot h_r = h$ and $\tilde{h}_p \cdot h_r \vDash p * r$, so that, from Assumption 4, and (1) for the definition of best$(p * r, q * r)$ (taking h_p to be $\tilde{h}_p \cdot h_r$ and renaming h'_q to $\tilde{h}'_{qr}$), we know that there is an $\tilde{h}'_{qr}$ such that

$$h' = \tilde{h}'_{qr} \cdot (h - \tilde{h}_p \cdot h_r) = \tilde{h}'_{qr} \cdot (h_0 - \tilde{h}_p) \text{ and } \tilde{h}'_{qr} \vDash q * r.$$

Then, since $h'_r \vDash_{\min} r$ and both h'_r and $\tilde{h}'_{qr}$ are subsets of h', by Part 4 of Proposition 17 we have $\tilde{h}'_{qr} = h'_r \cdot (\tilde{h}'_{qr} - h'_r)$ and $\tilde{h}'_{qr} - h'_r \vDash q$. Thus, we can define $\tilde{h}'_q$ to be $\tilde{h}'_{qr} - h'_r$, and obtain $h' = \tilde{h}'_{qr} \cdot (h_0 - \tilde{h}_p) = \tilde{h}'_q \cdot h'_r \cdot (h_0 - \tilde{h}_p)$, so that $h'_0 = \tilde{h}'_q \cdot (h_0 - \tilde{h}_p)$.