Definition 1 ($\tau - Equal$ Memories)**.** *Two memories μ_0, μ_1 are $\tau - Equal$ for Γ, written $\mu_0 =^{\Gamma}_{\tau} \mu_1$,* iff *$dom(\mu_0) = dom(\mu_1) \wedge \forall x \in \mu_0$ such that* if $\Gamma(\mathsf{x}) = \tau'\ \mathsf{var} \wedge \tau' \leq \tau$*, then $\mu_0(x) = \mu_1(x)$.*

Definition 2 (Filtering)**.** *Let* $\mathsf{filter}_{\tau}(\mathsf{t}) = \mathsf{filter}'_{\tau}(\mathsf{t}, [\,])$ *and* $\mathsf{filter}'_{\tau}([\,], \mathsf{t}) = \mathsf{t}$.

$$\mathsf{filter}'_{\tau}(\mathsf{BEnc}(\mathsf{L}, \mathsf{vk}, \mathsf{v}'||\mathsf{v}) \cdot \mathsf{t}', \mathsf{t}) = \begin{cases} \mathsf{filter}'_{\tau}(\mathsf{t}', \mathsf{t} \cdot (\mathsf{L}, \mathsf{v}')) & \text{if } \Gamma(\mathsf{L}) \leq \tau \\ \mathsf{filter}'_{\tau}(\mathsf{t}', \mathsf{t}) & Otherwise \end{cases}$$

Definition 3 (NonInterference)**.** *A server program p is NI at τ for Γ, written $NI^{\Gamma}_{\tau}(p)$,* iff *$\forall \mu_0, \mu_1$ such that $\mu_0 =^{\Gamma}_{\tau} \mu_1 \wedge \mu_0 \vdash p \Rightarrow^{t_0} \mu'_0 \wedge \mu_1 \vdash p \Rightarrow^{t_1} \mu'_1$, then $\mu'_0 =^{\Gamma}_{\tau} \mu'_1 \wedge \mathsf{filter}(\mathsf{t}_0) = \mathsf{filter}(\mathsf{t}_1)$.*

Lemma 1. *(LowExpression) $\forall \tau, \tau', \mu_0, \mu_1$, if $\mu_0 =^{\Gamma}_{\tau} \mu_1$ and $\Gamma \vdash e : \tau'$ and $\tau' \leq \tau$ and $\mu_0 \vdash e \Rightarrow v_0$ and $\mu_1 \vdash e \Rightarrow v_1$, then $v_0 = v_1$.*

Theorem 1. *If $\Gamma \vdash p$ then p is NI^{Γ}_{τ}.*

Proof. By Definition 3, for p to be NI^{Γ}_{τ}, we need to prove that:

(G_1) $\mu'_0 =^{\Gamma}_{\tau} \mu'_1$.

(G_2) $\mathsf{filter}_{\tau}(\mathsf{t}_0) = \mathsf{filter}_{\tau}(\mathsf{t}_1)$.

We prove this theorem by induction on the height of typing derivation tree $\Gamma \vdash p$.

Case 1. *Base case: height = 2*

Subcase 1.1. $p \overset{\Delta}{=} x := e'$.

Concerning (G_1) and (G_2), by Definition 3, we have that:

(H_1) $\mu_0 =^{\Gamma}_{\tau} \mu_1$.

(H_2) $\mu_i \vdash x := e' \Rightarrow^{t_i} \mu'_i$.

Moreover, for the semantics rule Update we have that:

(H_3) $t_i = \varepsilon$.

Hence, by the semantics rule Update and (H_2), we have that:

(H_4) $\mu_i \vdash e' \Rightarrow v_i$.

(H_5) $\mu'_i = \mu_i[x := v_i]$.

By the hypothesis of Theorem 1, we have:

(H_6) $\Gamma \vdash x := e' : \tau'\ cmd$.

By (H_6) and the typing rule Assign, we have that:

(H_7) $\Gamma \vdash x : \tau'\ var$.

(H_8) $\Gamma \vdash e' : \tau'$.

By (H_7) and the typing rule Var, we have:

(H_9) $\Gamma(x) = \tau'$ *var*.

Depending on τ', we have two cases:

(H_{10}) $\tau' \leq \tau$.

By Lemma 1 that can be applied due to (H_1), (H_8), (H_{10}) and (H_4) then $(H_{11}):\ v_0 = v_1$.
To prove (G_1), we rely on the Definition 1 that states that $\mu_0 =^{\Gamma}_{\tau} \mu_1$, if $\forall x \in \mu_0$ such that $\Gamma(x) = \tau'$ *var* and $\tau' \leq \tau$ then $\mu_0(x) = \mu_1(x)$.
Since (H_1) holds and the only variable in which μ_i and μ'_i are different is x by (H_5), then we need to prove that $\mu_0(x) = \mu_1(x)$ which holds by (H_{11}).
To prove (G_2) we rely on the Definition 2 and (H_3). Since $t_0 = t_1 = \varepsilon$ then $\mathsf{filter}_{\tau}(\mathsf{t}_0) = \mathsf{filter}_{\tau}(\mathsf{t}_1)$.

Since we proved (G_1) and (G_2), then p is NI^{Γ}_{τ}.

(H_{12}) $\tau' \not\leq \tau$.

To prove (G_1), we rely on the Definition 1 that states that $\mu_0 =^{\Gamma}_{\tau} \mu_1$, if $\forall y \in \mu_0$ such that $\Gamma(y) = \tau'$ *var* and $\tau' \leq \tau$ then $\mu_0(s) = \mu_1(y)$. For (H_{12}), we have that $\tau' \not\leq \tau$. Since we are only interested by variables with security level less or equal than τ, we can conclude by (H_5) and (H_1) that $\mu'_0 =^{\Gamma}_{\tau} \mu'_1$.

To prove (G_2) we rely on the Definition 2 and (H_3). Since $t_0 = t_1 = \varepsilon$ then $\mathsf{filter}_{\tau}(\mathsf{t}_0) = \mathsf{filter}_{\tau}(\mathsf{t}_1)$.

Since we proved (G_1) and (G_2), then p is NI^{Γ}_{τ}.

Subcase 1.2. $p \overset{\Delta}{=} \mathsf{pc} := \mathsf{pc} + 1$.
Concerning (G_1) and (G_2), by Definition 3, we have that:

(H_1) $\mu_0 =^{\Gamma}_{\tau} \mu_1$.

(H_2) $\mu_i \vdash \mathsf{pc} := \mathsf{pc} + 1 \Rightarrow^{\mathsf{t_i}} \mu'_{\mathsf{i}}$.

By the semantics rule Update we have that:

(H_3) $t_i = \varepsilon$.

Moreover, by the semantics rule Update and (H_2), we have that:

(H_4) $\mu_i \vdash \mathsf{pc} + 1 \Rightarrow \mathsf{v_i}$.

(H_5) $\mu'_i = \mu_i[x := v_i]$.

By the hypothesis of Theorem 1, we have:

(H_6) $\Gamma \vdash \mathsf{pc} := \mathsf{pc} + 1 : \bot\ \mathsf{cmd}$.

By the typing rule Assign-Counter, we have that:

(H_7) $\Gamma \vdash \mathsf{pc} : \bot\ \mathsf{Cvar}$.

To prove (G_1), we rely on the Definition 1 that states that $\mu_0 =^{\Gamma}_{\tau} \mu_1$*, if* $\forall y \in \mu_0$ *such that* $\Gamma(y) = \tau'$ *var and* $\tau' \leq \tau$ *then* $\mu_0(y) = \mu_1(y)$*. For (H_7),* $\Gamma(\mathsf{pc}) = \bot\ \mathsf{Cvar}$*. Since we are only interested in variables of type* τ' *var, we conclude by (H_5) and (H_1) that* $\mu'_0 =^{\Gamma}_{\tau} \mu'_1$.

To prove (G_2) we rely on the Definition 2 and (H_3)*. Since* $t_0 = t_1 = \varepsilon$ *then* $\mathsf{filter}_{\tau}(\mathsf{t}_0) = \mathsf{filter}_{\tau}(\mathsf{t}_1)$.

Since we proved (G_1) and (G_2), then p is NI^{Γ}_{τ}.

Subcase 1.3. $p \triangleq \mathsf{sbroadcast}(\mathsf{L}, \mathsf{e}||\mathsf{pc}, \mathsf{K})$.

Concerning (G_1) and (G_2), by Definition 3, we have that:

(H_1) $\mu_0 =^{\Gamma}_{\tau} \mu_1$.

(H_2) $\mu_i \vdash \mathsf{sbroadcast}(\mathsf{L}, \mathsf{e}||\mathsf{pc}, \mathsf{K}) \Rightarrow^{\mathsf{t_i}} \mu_{\mathsf{i}}$.

By the semantics rule Secure Broadcast, we have:

(H_3) $t_i = \mathsf{BEnc}(\mathsf{L}, \mathsf{vk_i}, \text{"m"}||\text{"v"})$.

(H_4) $\mu_i \vdash K \Rightarrow v'_i$.

(H_5) $\mu_i \vdash e \Rightarrow \text{"}m_i\text{"}$.

(H_6) $\mu_i \vdash \mathsf{pc} \Rightarrow \mathsf{v_i}$.

(H_7) $\mu_i(L) = \{\text{"}n_0\text{"}, \text{"}n_1\text{"}, \ldots, \text{"}n_n\text{"}\}$.

By the hypothesis of Theorem 1, we have:

(H_8) $\Gamma \vdash \mathsf{sbroadcast}(\mathsf{L}, \mathsf{e}||\mathsf{pc}, \mathsf{K}) : \tau\ \mathsf{cmd}$.

By (H_8) and the typing rule SBroadcast, we have:

(H_9) $\Gamma \vdash e : \tau$.

(H_{10}) $\Gamma \vdash L : \tau\ Lvar$.

(H_{11}) $\Gamma \vdash K : \top\ Kvar$.

(H_{12}) $\Gamma \vdash \mathsf{pc} : \bot\ \mathsf{Cvar}$.

To prove (G_1), we rely on the Definition 1 that states that $\mu_0 =^{\Gamma}_{\tau} \mu_1$*, if* $\forall y \in \mu_0$ *such that* $\Gamma(y) = \tau'$ *var and* $\tau' \leq \tau$ *then* $\mu_0(y) = \mu_1(y)$*. For ($H_9 - H_{12}$), all the variables types are different than* τ' *var. Since we are only interested in variables of type* τ' *var, (G_1) follows by (H_1) and (H_2).*

To prove (G_2), we have two cases:

(H_{13}) $\Gamma(L) \leq \tau$

Being $\mu'_0 =^{\Gamma}_{\tau} \mu'_1$ *and by (*H_2*) and(*H_3*) we have that* $t_0 = t_1$*. For an execution that starts with* μ_0*,* $t_0 = \mathsf{BEnc}(\mathsf{L}, \mathsf{vk_0}, \text{"m"}||\text{"v"})$ *and for an execution that starts with* μ_1*,* $t_1 = \mathsf{BEnc}(\mathsf{L}, \mathsf{vk_1}, \text{"m"}||\text{"v"})$*. By (*$H_{13}$*),* $\Gamma(L) \leq \tau$ *then* $\mathsf{filter}(\mathsf{t_0}) = [\mathsf{L}, \mathsf{m}]$ *and* $\mathsf{filter}(\mathsf{t_1}) = [\mathsf{L}, \mathsf{m}]$*. It results that* $\mathsf{filter}(\mathsf{t_0}) = \mathsf{filter}(\mathsf{t_1})$ *and therefore we prove (*G_2*).*

Since we proved (G_1*) and (*G_2*), then p is* NI^{Γ}_{τ}.

(H_{14}) $\Gamma(L) \not\leq \tau$

Being $\mu'_0 =^{\Gamma}_{\tau} \mu'_1$ *and by (*H_2*) and(*H_3*) we have that* $t_0 = t_1$*. For an execution that starts with* μ_0*,* $t_0 = \mathsf{BEnc}(\mathsf{L}, \mathsf{vk_0}, \text{"m"}||\text{"v"})$ *and for an execution that starts with* μ_1*,* $t_1 = \mathsf{BEnc}(\mathsf{L}, \mathsf{vk_1}, \text{"m"}||\text{"v"})$*. By (*$H_{14}$*),* $\Gamma(L) \not\leq \tau$*, then* $\mathsf{filter_\tau}(\mathsf{t_0}) = [\,]$ *and* $\mathsf{filter_\tau}(\mathsf{t_1}) = [\,]$*. It results that* $\mathsf{filter_\tau}(\mathsf{t_0}) = \mathsf{filter_\tau}(\mathsf{t_1})$ *and therefore we prove (*G_2*).*

Since we proved (G_1*) and (*G_2*), then p is* NI^{Γ}_{τ}.

Subcase 1.4. $p \overset{\Delta}{=} \mathsf{for\ n \in L\ endorse\ Ra(L, L', n)}$.

Concerning (G_1*) and (*G_2*), by Definition 3, we have that:*

(H_1) $\mu_0 =^{\Gamma}_{\tau} \mu_1$.

(H_2) $\mu_i \vdash \mathsf{for\ n \in L\ endorse\ Ra(L, L', n)} \Rightarrow^{\mathsf{t_i}} \mu'_{\mathsf{i}}$.

By the semantics rule Endorse-Ra we have that:

(H_3) $t_i = \varepsilon$.

(H_4) $\mu_i \vdash \mathsf{Ra(L)} \Rightarrow \mathsf{S}$.

(H_5) $\mu_i(L) = \{\text{"}n_0\text{"}, \text{"}n_1\text{"}, ..., \text{"}n_n\text{"}\}$.

(H_6) $\mu_i(L') = \{\text{"}n'_0\text{"}, \text{"}n'_1\text{"}, ..., \text{"}n'_n\text{"}\}$.

By (H_2*) and the semantics rule Endorse-Ra we have that:*

(H_7) $\mu'_i = \mu_i[L := L\ S; L' := L' \cup S]$.

By the hypothesis of Theorem 1, we have:

(H_8) $\Gamma \vdash \mathsf{for\ n \in L\ endorse\ Ra(L, L', n)} : \tau\ \mathsf{cmd}$.

By (H_8*) and the typing rule Remote Attestation, we have that:*

(H_9) $\Gamma \vdash L : \tau\ Lvar$.

(H_{10}) $\Gamma \vdash L' : \tau'\ Lvar$.

(H_{11}) $\Gamma \vdash K : \top\ Kvar$.

(H_{12}) $\Gamma \vdash \mathsf{pc} : \bot\ \mathsf{Cvar}$.

To prove (G_1), we rely on the Definition 1 that states that $\mu_0 =^{\Gamma}_{\tau} \mu_1$, if $\forall y \in \mu_0$ such that $\Gamma(y) = \tau'$ var and $\tau' \leq \tau$ then $\mu_0(y) = \mu_1(y)$. For ($H_9 - H_{12}$), all the variables types are different than τ' var. Since we are only interested in variables of type τ' var, (G_1) follows by (H_1) and (H_2).

To prove (G_2) we rely on the Definition 2 and (H_3). Since $t_0 = t_1 = \varepsilon$ then $\mathsf{filter}_{\tau}(\mathsf{t}_0) = \mathsf{filter}_{\tau}(\mathsf{t}_1)$.

Since we proved (G_1) and (G_2), then p is NI^{Γ}_{τ}.

Case 2. *Case: height $\leq n$ We will state our inductive hypothesis for a program c:*

For the hypothesis of the theorem, we have that:

(IH_1) $\Gamma \vdash c : \tau\ cmd$.

(IH_2) $\mu_0 =^{\Gamma}_{\tau} \mu_1$.

For the derivation tree of height $\leq n$, we have that:

(IH_3) $\mu_0 \vdash c \Rightarrow^{t_0} \mu'_0$.

(IH_4) $\mu_1 \vdash c \Rightarrow^{t_1} \mu'_1$.

Then we conclude that:

(IH_5) $\mu'_0 =^{\Gamma}_{\tau} \mu'_1$.

(IH_6) $\mathsf{filter}_{\tau}(\mathsf{t}_0) = \mathsf{filter}_{\tau}(\mathsf{t}_1)$.

We suppose that ($IH_1 - IH_6$) are valid for programs of height $\leq n$ of typing derivation tree $\Gamma \vdash p$.

Case 3. *Inductive case: height$= n+1$*

Subcase 3.1. $p \triangleq c';c''$.

We want to prove that $\Gamma \vdash c';c''$ is NI^{Γ}_{τ}. We assume that c' and c'' are of height $\leq n$, and $c';c''$ of height $n+1$.

For the typing rule Sequence, we have that:

(H_1) $\Gamma \vdash c' : \tau\ cmd$.

(H_2) $\Gamma \vdash c'' : \tau\ cmd$.

For the semantics rule Sequence, we have that:

(H_3) $\mu_i \vdash c' \Rightarrow^{t'_i} \mu'_i$.

(H_4) $\mu'_i \vdash c'' \Rightarrow^{t''_i} \mu''_i$.

Concerning c', from the inductive hypotheses, it follows that:

(H_5) $\mu_{c'_0} =^{\Gamma}_{\tau} \mu_{c'_1}$.

(H_6) $\mu_{c'_0} \vdash c \Rightarrow^{t'_0} \mu'_{c'_0}$

(H_7) $\mu_{c'_1} \vdash c \Rightarrow^{t'_1} \mu'_{c'_1}$

(H_8) $\mu'_{c'_0} =^{\Gamma}_{\tau} \mu'_{c'_1}$.

(H_9) $\mathsf{filter}_\tau(\mathsf{t}'_0) = \mathsf{filter}_\tau(\mathsf{t}'_1)$.

It follows that c' is NI^{Γ}_{τ}.

Concerning c'', from the inductive hypotheses, it follows that:

(H_{10}) $\mu_{c''_0} =^{\Gamma}_{\tau} \mu_{c''_1}$.

(H_{11}) $\mu_{c''_0} \vdash c \Rightarrow^{t''_0} \mu'_{c''_0}$

(H_{12}) $\mu_{c''_1} \vdash c \Rightarrow^{t''_1} \mu'_{c''_1}$

(H_{13}) $\mu'_{c''_0} =^{\Gamma}_{\tau} \mu'_{c''_1}$.

(H_{14}) $\mathsf{filter}_\tau(\mathsf{t}''_0) = \mathsf{filter}_\tau(\mathsf{t}''_1)$.

It follows that c'' is NI^{Γ}_{τ}.

In the semantics rule Sequence, we use $t' \cdot t''$ to denote the concatenation of two traces t' and t''. By (H_9) and (H_{14}) we have that $t'_0 = t'_1$ and $t''_0 = t''_1$, which implies that $t'_0 \cdot t''_0 = t'_1 \cdot t''_1$. We conclude that $\mathsf{filter}_\tau(\mathsf{t}'_0 \cdot \mathsf{t}''_0) = \mathsf{filter}_\tau(\mathsf{t}'_1 \cdot \mathsf{t}''_1)$.

Since c', c'' are NI^{Γ}_{τ} and $\mathsf{filter}_\tau(\mathsf{t}'_0 \cdot \mathsf{t}''_0) = \mathsf{filter}_\tau(\mathsf{t}'_1 \cdot \mathsf{t}''_1)$*, we conclude that $\Gamma \vdash c';c''$ is NI^{Γ}_{τ}.*

Subcase 3.2. $p \triangleq \mathsf{while\ e\ do\ c'}$.

For the typing rule While, we have that:

(H_1) $\Gamma \vdash c' : \tau'$ *cmd.*

(H_2) $\Gamma \vdash e : \tau'$.

In the following, we show by induction that c' is NI^{Γ}_{τ}.

By (H_1) and because the height of $\Gamma \vdash \mathsf{while\ e\ do\ c'}$ *is $n+1$, we know that the height of the typing derivation tree of (H_1) is $\leq n$. Hence, we can apply the inductive hypothesis and get:*

(H_3) $\mu_0 =^{\Gamma}_{\tau} \mu_1$.

(H_4) $\mu_0 \vdash c' \Rightarrow^{t_0} \mu'_0$.

(H_5) $\mu_1 \vdash c' \Rightarrow^{t_1} \mu'_1$.

Then,

(H_6) $\mu'_0 =^{\Gamma}_{\tau} \mu'_1$.

(H_7) $\mathsf{filter}_\tau(\mathsf{t}_0) = \mathsf{filter}_\tau(\mathsf{t}_1)$.

We want to prove that $\mathsf{while\ e\ do\ c'}$ *is* NI^{Γ}_{τ}. *By the hypothesis of the theorem, we have that if:*

(H'_0) $\Gamma \vdash \mathsf{while\ e\ do\ c'} : \tau'\ \mathsf{cmd}$.

(H'_1) $\mu_0 =^{\Gamma}_{\tau} \mu_1$.

(H'_2) $\mu_0 \vdash \mathsf{while\ e\ do\ c} \Rightarrow^{\mathsf{t}_0} \mu'_0$.

(H'_3) $\mu_1 \vdash \mathsf{while\ e\ do\ c} \Rightarrow^{\mathsf{t}_1} \mu'_1$.

Then, we want to prove that:

(G_0) $\mu'_0 =^{\Gamma}_{\tau} \mu'_1$.

(G_1) $\mathsf{filter}_{\tau}(\mathsf{t}_0) = \mathsf{filter}_{\tau}(\mathsf{t}_1)$.

By (H'_2) and the semantics rule of Loop, we have that:

(H'_4) $\mu_0 \vdash e \Rightarrow v_0$.

By (H'_3) and the semantics rule of Loop, we have that:

(H'_5) $\mu_1 \vdash e \Rightarrow v_1$.

Depending on τ'*, we have two cases:*

Subcase 3.2.1. $\Gamma \vdash e : \tau'$, $\tau' \leq \tau$.

(H'_6) $\tau' \leq \tau$.

By Lemma 1 that can be applied on (H'_1), (H_2), (H'_6), (H'_4) and (H'_5), we conclude that $v_0 = v_1$.

We prove this case by induction on the height of the semantics tree of (H'_2). (We do not show this formally, but we rely on the fact that the height of (H'_2) is equal to the height of (H'_3) by Lemma 1).

Base case: height = 2. *The only possibility for the semantics tree to be of height* $= 2$ *is:*

- $v_0 = v_1 = False$.

$$\frac{\mu_0 \vdash e \Rightarrow False}{\mu_0 \vdash \mathsf{while\ e\ do\ c} \Rightarrow^{\mathsf{t}_0} \mu_0}$$

$$\frac{\mu_1 \vdash e \Rightarrow False}{\mu_1 \vdash \mathsf{while\ e\ do\ c} \Rightarrow^{\mathsf{t}_1} \mu_1}$$

We have that $\mu'_0 = \mu_0$ *and* $\mu'_1 = \mu_1$. *We conclude by (H'_1) that* $\mu'_0 =^{\Gamma}_{\tau} \mu'_1$. *Moreover, since* $t_0 = t_1 = \varepsilon$ *then* $\mathsf{filter}_{\tau}(\mathsf{t}_0) = \mathsf{filter}_{\tau}(\mathsf{t}_1)$.

Assuming that our inductive hypothesis holds for the case of While when evaluating the height of semantics tree $\leq m$ *with* $\Gamma \vdash e : \tau', \tau' \leq \tau$, *let us prove the case of While with height* $= m+1$.

Inductive case: height = m+1.

$$\frac{\mu_0 \vdash e \Rightarrow \mathit{True} \qquad \mu_0 \vdash c' \Rightarrow^{t_0} \mu_0'' \qquad (H_7')\ \mu_0'' \vdash \mathsf{while\ e\ do\ c'} \Rightarrow^{\mathsf{t}_0'} \mu_0'}{\mu_0 \vdash \mathsf{while\ e\ do\ c'} \Rightarrow^{\mathsf{t}_0 \cdot \mathsf{t}_0'} \mu_0'}$$

The height of (H_2') is $m+1$.

$$\frac{\mu_1 \vdash e \Rightarrow \mathit{True} \qquad \mu_1 \vdash c' \Rightarrow^{t_1} \mu_1'' \qquad (H_8')\ \mu_1'' \vdash \mathsf{while\ e\ do\ c'} \Rightarrow^{\mathsf{t}_1'} \mu_1'}{\mu_1 \vdash \mathsf{while\ e\ do\ c'} \Rightarrow^{\mathsf{t}_1 \cdot \mathsf{t}_1'} \mu_1'}$$

The height of (H_3') is $m+1$.

By the previous induction on c', *we have that* $\mu_0'' =_\tau^\Gamma \mu_1''$ *and* $\mathsf{filter}_\tau(\mathsf{t}_0) = \mathsf{filter}_\tau(\mathsf{t}_1)$, *through* $\mu_0 =_\tau^\Gamma \mu_1$, $\mu_0 \vdash c' \Rightarrow^{t_0} \mu_0''$ *and* $\mu_1 \vdash c' \Rightarrow^{t_1} \mu_1''$.

Moreover, by induction on while e do c′ *by* (H_7') *and* (H_8'), *we can conclude that* $\mu_0' =_\tau^\Gamma \mu_1'$ *which is already our goal* (G_1) *and* $\mathsf{filter}_\tau(\mathsf{t}_0') = \mathsf{filter}_\tau(\mathsf{t}_1')$. *This is because we have that* $\mu_0'' =_\tau^\Gamma \mu_1''$ *and* $\mu_0'' \vdash \mathsf{while\ e\ do\ c'} \Rightarrow^{\mathsf{t}_0'} \mu_0'$ *and* $\mu_1'' \vdash \mathsf{while\ e\ do\ c'} \Rightarrow^{\mathsf{t}_1'} \mu_1'$.

Since $t_i \cdot t_i'$ *is the concatenation of two traces* t_i *and* t_i', *and since* $\mathsf{filter}_\tau(\mathsf{t}_0) = \mathsf{filter}_\tau(\mathsf{t}_1)$ *and* $\mathsf{filter}_\tau(\mathsf{t}_0') = \mathsf{filter}_\tau(\mathsf{t}_1')$, *we conclude that* $\mathsf{filter}_\tau(\mathsf{t}_0 \cdot \mathsf{t}_0') = \mathsf{filter}_\tau(\mathsf{t}_1 \cdot \mathsf{t}_1')$ *from which* (G_2) *follows.*

Since (G_1) *and* (G_2) *are satisfied, then* while e do c′ *is* NI_τ^Γ.

Subcase 3.2.2. $\Gamma \vdash e : \tau'$, $\tau' \not\leq \tau$.

Lemma 2. *(HighCommand)* $\forall \tau, \tau', \mu_i$, *if* $\Gamma \vdash c : \tau'$ *cmd and* $\tau' \not\leq \tau$ *and* $\mu_i \vdash c \Rightarrow \mu_i'$, *then* $\mu_i =_\tau^\Gamma \mu_i'$

□