Online Appendix to: On Protection by Layout Randomization

MARTÍN ABADI, Microsoft Research, Silicon Valley; University of California,
Santa Cruz; Collège de France

GORDON D. PLOTKIN, Microsoft Research, Silicon Valley; LFCS, Informatics,
University of Edinburgh

We present the proofs of the main theorems and preliminary results needed for those proofs. We often omit or abbreviate proofs when they are routine.

A. THE FATAL-ERROR MODEL

A.1. The High-Level Language

There is a small-step subject-reduction theorem for the high-level semantics.

LEMMA A.1. *For any configuration (s, M) , with $M : \sigma$, one of the following three mutually exclusive statements holds:*

- M is a value,
- $(s, M) \longrightarrow (s', M')$ for some uniquely determined s' and $M' : \sigma$, or
- $(s, M) \downarrow_{\text{error}}$.

This lemma yields a big-step subject-reduction theorem.

LEMMA A.2. *For any configuration (s, M) , with $M : \sigma$, one of the following three mutually exclusive statements holds:*

- $(s, M) \Longrightarrow (s', V)$ for a unique s' and $V : \sigma$,
- $(s, M) \downarrow_{\text{error}}$, or
- $(s, M) \uparrow$.

A.2. The Low-Level Language

The small-step subject-reduction theorem for the low-level language is as follows.

LEMMA A.3. *For any memory layout w and configuration (m, M) , with $M : \sigma$, one of the following four mutually exclusive statements holds:*

- M is a value,
- $w \models (m, M) \longrightarrow (m', M')$ for some uniquely determined m' and $M' : \sigma$, and if m has the form s_w , so does m' ,
- $w \models (m, M) \downarrow_{\text{error}}$, or
- $w \models (m, M) \downarrow_{\text{error}}^a$ for some uniquely determined a .

The corresponding big-step subject-reduction theorem is as follows.

LEMMA A.4. *For any memory layout w and configuration (m, M) , with $M : \sigma$, one of the following four mutually exclusive statements holds:*

- $w \models (m, M) \Longrightarrow (m', V)$ for a unique m' and $V : \sigma$, and if m has the form s_w , so does m' ,
- $w \models (m, M) \downarrow_{\text{error}}$,

- $w \models (m, M) \Downarrow_{\text{error}}^a$ for some uniquely determined a , or
- $w \models (m, M) \Uparrow$.

A.3. The Instrumented High-Level Language

For the analogue to Lemma A.1, one adds one more possibility to the list of mutually exclusive possibilities:

- $(s, M) \Downarrow_{\text{error}}^a$ for some uniquely determined a .

and, for the analogue of Lemma A.2 one adds the following possibility to the list of mutually exclusive possibilities:

- $(s, M) \Downarrow_{\text{error}}^a$ for some unique a .

A.3.1. Translating Instrumented High-Level to High-Level. The translation is correct for the small-step semantics, in the following sense (where $(s, M) \Downarrow_{\text{error}}^u$ holds if, and only if, either $(s, M) \Downarrow_{\text{error}}$ or $(s, M) \Downarrow_{\text{error}}^a$ for some a).

LEMMA A.5. *Let M be a well-typed term of the instrumented high-level language. Then:*

- (1) *If M is a value then so is $M^\dagger$.*
- (2) *If $(s, M) \longrightarrow (s', M')$ then $(s, M^\dagger) \longrightarrow^* (s', (M')^\dagger)$.*
- (3) *If $(s, M) \Downarrow_{\text{error}}^u$ then $(s, M^\dagger) \longrightarrow^* (s, M') \Downarrow_{\text{error}}$ for some M' .*

PROOF. Part 1 follows by inspection. For part 2, one shows first that, for any redex R , if $(s, R) \longrightarrow (s', M')$ then $(s, R^\dagger) \longrightarrow^* (s', (M')^\dagger)$. One shows next that, if E is an evaluation context, then $E^\dagger$ is too (taking $[-]^\dagger = [-]$, etc.) and $E[M]^\dagger = E^\dagger[M^\dagger]$. Part 2 then follows. For part 3, one shows first that, for any redex R , if $(s, R) \Downarrow_{\text{error}}^u$ then $(s, R^\dagger) \longrightarrow^* (s, M') \Downarrow_{\text{error}}$ for some M' , and then applies the previous remark on evaluation contexts. $\square$

Proposition 4.1, the corresponding translation-correctness result for the big-step semantics, is an immediate consequence of this lemma.

A.3.2. Translating Instrumented High-Level to Low-Level. A series of lemmas leads to the main simulation results. The first lemma concerns values.

LEMMA A.6. *Suppose that $V \searrow_w N$ for a well-typed value V . Then for some V' with $V \searrow_w V'$, we have, for any m , $w \models (m, N) \longrightarrow^* (m, V')$.*

The second lemma concerns redexes.

LEMMA A.7. *Suppose that $R \searrow_w N$ and that $(s, R) \longrightarrow (s', M')$. Then for some N' with $M' \searrow_w N'$ we have $w \models (s_w, N) \longrightarrow^* (s'_w, N')$.*

PROOF. The proof is straightforward. The case where $R \longrightarrow M'$ makes use of Lemma A.6. For example, suppose that R is $\text{fst}(V, V')$. Then, N has the form $\text{fst}(N_1, N'_1)$ where $V \searrow_w N_1$ and $V' \searrow_w N'_1$. Applying Lemma A.6 twice, we then have that:

$$(s_w, \text{fst}(N_1, N'_1)) \longrightarrow (s_w, \text{fst}(V_1, V'_1)) \longrightarrow (s_w, V_1)$$

for some values V_1, V'_1 with $V \searrow_w V_1$ and $V' \searrow_w V'_1$. $\square$

The third lemma concerns evaluation contexts. The simulation relation is extended in an evident way to evaluation contexts, taking, $[-] \searrow_w [-]$, etc. One easily sees that if $E \searrow_w E'$ and $M \searrow_w N$ then $E[M] \searrow_w E'[N]$.

LEMMA A.8. *Suppose that $E[R] \searrow_w N$. Then, N has the form $E'[N_1]$ where $E \searrow_w E'$ and $R \searrow_w N_1$.*

We now have a small-step simulation lemma.

LEMMA A.9. *Suppose that $M \searrow_w N$ for a well-typed terms M of the instrumented high-level language and N of the low-level language. Then:*

- (1) *If M is a value, then there is a V' , with $M \searrow_w V'$, such that for any m , $w \models (m, N) \longrightarrow^* (m, V')$.*
- (2) *If $(s, M) \longrightarrow (s', M')$, then there is an N' , with $M' \searrow_w N'$, such that $w \models (s_w, N) \longrightarrow^* (s'_w, N')$.*
- (3) *If $(s, M) \downarrow_{\text{error}}$, then $w \models (s_w, N) \downarrow_{\text{error}}$.*
- (4) *If $(s, M) \downarrow_{\text{error}}^a$, then, if $a \notin \text{Ran}(w)$, $w \models (s_w, N) \downarrow_{\text{error}}^a$.*

PROOF. The first part is an immediate consequence of Lemma A.6, as is the second part of Lemmas A.7 and A.8. For the third and fourth parts, one verifies the assertions when M is a redex, and then applies Lemma A.8. $\square$

Proposition 4.2, the corresponding big-step simulation result, is an immediate consequence of this lemma.

A.4. High and Low-Level Attackers

PROOF OF PROPOSITION 4.3. That these are all the possibilities is simply because CM is a high-level term. That the statements concerning these possibilities hold is an immediate consequence of Proposition 4.2. (Note that, for any value $V : \text{bool}$, if $V \searrow_w V'$ then $V' = V$.) $\square$

PROOF OF THEOREM 4.5. First note that $(CM)^\uparrow = C^\uparrow M^\uparrow = C^\uparrow M$ (as $M^\uparrow = M$) and also that $(CM)^\downarrow = C^\downarrow M^\downarrow = CM^\downarrow$ (as $C^\downarrow = C$). The proof now proceeds by considering the big-step behavior of (s, CM) . There are four mutually exclusive possibilities: we consider each of them in turn.

(1) In the first case, we have $(s, CM) \implies (s', V)$ for some s' and V . We then have $(s, C^\uparrow M) \implies (s', V)$, by part 1 of Proposition 4.1. Using part 1 of Proposition 4.2, we also have, for any w that $w \models (s_w, CM^\downarrow) \implies (s'_w, V')$, for some V' with $V \searrow_w V'$; as V is a Boolean value, we then have that V and V' are identical.

(2) In the second case, we have $(s, CM) \downarrow_{\text{error}}$, so, arguing as before, but here using the second parts of the propositions, $(s, C^\uparrow M) \downarrow_{\text{error}}$ and, for any w , $w \models (s, CM^\downarrow) \downarrow_{\text{error}}$ (as $M \searrow_w M^\downarrow$). We therefore have:

$$P(w \models (s_w, CM^\downarrow) \downarrow_{\text{error}}^u) \geq P(w \models (s_w, CM^\downarrow) \downarrow_{\text{error}}) = 1 \geq \delta_1.$$

(3) In the third case we have $(s, CM) \downarrow_{\text{error}}^a$, for some $a \geq 0$ with $a \notin \text{Ran}(w_p)$. So, again arguing as before, but here using the second and third parts of the propositions, respectively, we have that $(s, C^\uparrow M) \downarrow_{\text{error}}^a$, and that, for any w with $a \notin \text{Ran}(w)$, $w \models (s_w, CM^\downarrow) \downarrow_{\text{error}}$. It follows that:

$$P(w \models (s_w, CM^\downarrow) \downarrow_{\text{error}}^a) \geq P(w \# \{a\}) \geq \delta_1$$

(4) The fourth case is similar to the first case, but uses the third and fourth parts of the respective propositions. $\square$

Note how, in this proof, the behavior of a term CM of the instrumented high-level language is used to coordinate the behaviors of terms $C^\uparrow M$ and $CM^\downarrow$ of the high- and low-level languages, respectively.

A.5. Equivalences

PROOF OF THEOREM 4.7. In one direction, we assume that σ is loc-free, so that $\sigma^\downarrow = \sigma$, and $M \approx_{h,p} N$, and then consider a public low-level term $C : \sigma \rightarrow \text{bool}$ in order to show $CM^\downarrow \sim_{l,p} CN^\downarrow$. Choose a store s . From the assumption that $M \approx_{h,p} N$ we then obtain $\text{Eval}(C^\uparrow M, s) =_p \text{Eval}(C^\uparrow N, s)$, and three cases arise.

In the first case, we have that $(s, C^\uparrow M) \Rightarrow (s', V)$, $(s, C^\uparrow N) \Rightarrow (s'', V)$, and $s' \upharpoonright \text{PubLoc} = s'' \upharpoonright \text{PubLoc}$, for some s', s'' and V . Applying Theorem 4.5, we obtain that $w \models (s_w, CM^\downarrow) \Rightarrow (s'_w, V)$ and $w \models (s_w, CN^\downarrow) \Rightarrow (s''_w, V)$, for any w , which concludes this case.

In the second case, we have $(s, C^\uparrow M) \Downarrow_{\text{error}}$ and $(s, C^\uparrow N) \Downarrow_{\text{error}}$. Then, by Theorem 4.5, $P(w \models (s_w, C^\uparrow M) \Downarrow_{\text{error}}^u) \geq \delta_1$ and $P(w \models (s_w, C^\uparrow N) \Downarrow_{\text{error}}^u) \geq \delta_1$. The third case is similar to the first two.

For the converse, we assume $M^\downarrow \approx_{l,p} N^\downarrow$ and consider a public high-level term $C : \sigma \rightarrow \text{bool}$ in order to show that $\text{Eval}(CM, s) =_p \text{Eval}(CN, s)$, for any given store s . We know that $C^\downarrow M^\downarrow \sim_{l,p} C^\downarrow N^\downarrow$, and also, by Proposition 4.4, that, for all w , $\text{Eval}(CM, s)_w = \text{Eval}_w(C^\downarrow M^\downarrow, s_w)$ and $\text{Eval}(CN, s)_w = \text{Eval}_w(C^\downarrow N^\downarrow, s_w)$.

The definition of $\sim_{l,p}$ then yields three cases, of which the first and third are immediate. For the second, as $\delta_1 > 0$, we have $w_1 \models (s_{w_1}, C^\downarrow M^\downarrow) \Downarrow_{\text{error}}^u$ and $w_2 \models (s_{w_2}, C^\downarrow N^\downarrow) \Downarrow_{\text{error}}^u$, for some w_1 and w_2 , and the conclusion follows. $\square$

B. THE RECOVERABLE-ERROR MODEL

B.1. The High-Level Language

The small-step subject-reduction theorem is as follows.

LEMMA B.1. *For any configuration (s, M) , with $M : \sigma$, one of the following two mutually exclusive statements holds:*

- M is a value, or
- $(s, M) \longrightarrow (s', M')$ for some uniquely determined s' and $M' : \sigma$.

and the big-step subject-reduction theorem is:

LEMMA B.2. *For any configuration (s, M) , with $M : \sigma$, one of the following two mutually exclusive statements holds:*

- $(s, M) \Longrightarrow (s', V)$ for a unique s' and $V : \sigma$, or
- $(s, M) \Uparrow$.

B.2. The Low-Level Language

Here, the small-step subject-reduction theorem is as follows.

LEMMA B.3. *For any memory layout w and configuration (m, M) , with $M : \sigma$, one of the following three mutually exclusive statements holds:*

- M is a value,
- $w \models (m, M) \longrightarrow (m', M')$ for some uniquely determined m' and $M' : \sigma$, and if m has the form s_w , so does m' , or
- $w \models (m, M) \xrightarrow{a} (m', M')$ for some uniquely determined a, m' , and $M' : \sigma$, and if m has the form s_w , so does m' .

and the big-step subject-reduction theorem is the following.

LEMMA B.4. *For any configuration (m, M) , with $M : \sigma$, one of the following two mutually exclusive statements holds:*

- $w \models (m, M) \xrightarrow{A} (m', V)$ for a unique m' , $V : \sigma$, and $A \subseteq \mathbb{N}$, and if m has the form s_w , so does m' , or
- $w \models (m, M) \uparrow^A$ for a unique $A \subseteq \mathbb{N}$.

B.3. The Instrumented High-Level Language

For the analogue to Lemma B.1, one adds one more possibility to the list of mutually exclusive possibilities:

- $(s, M) \xrightarrow{a} (s', M')$ for some unique a, s' , and M' .

The big-step subject-reduction theorem is then as follows.

LEMMA B.5. *For any configuration (s, M) , with $M : \sigma$, one of the following two mutually exclusive statements holds:*

- $(s, M) \xrightarrow{A} (s', V)$ for a unique s' , $V : \sigma$, and $A \subseteq \mathbb{N}$, or
- $(s, M) \uparrow^A$ for a unique $A \subseteq \mathbb{N}$.

B.3.1. *Translating Instrumented High-Level to High-Level.* Proposition 5.1 follows from this small-step translation correctness result.

LEMMA B.6. *Let M be a well-typed term of the instrumented high-level language. Then:*

- (1) *If M is a value then so is $M^\uparrow$.*
- (2) *If $(s, M) \xrightarrow{A} (s', M')$ then $(s, M^\uparrow) \longrightarrow^* (s', (M')^\uparrow)$.*

PROOF. Part 1 follows by inspection. For part 2, one shows first that, for any redex R , if $(s, R) \xrightarrow{A} (s', M')$ then $(s, R^\uparrow) \longrightarrow^* (s', (M')^\uparrow)$. One shows next that if E is an evaluation context, then $E^\uparrow$ is too (taking $[-]^\uparrow = [-]$, etc.) and that $E[M]^\uparrow = E^\uparrow[M^\uparrow]$. Part 2 then follows. $\square$

B.3.2. *Translating Instrumented High-Level to Low-Level.* As before, a series of lemmas leads to the main simulation results.

LEMMA B.7. *Suppose that $V \searrow_w N$ for a well-typed value V . Then, for some V' with $V \searrow_w V'$, we have, for any m , $w \models (m, N) \longrightarrow^* (m, V')$.*

The second lemma concerns redexes.

LEMMA B.8.

- (1) *Suppose that $R \searrow_w N$ and that $(s, R) \longrightarrow (s', M')$. Then we have $w \models (s_w, N) \longrightarrow^* (s'_w, N')$ for some N' with $M' \searrow_w N'$.*
- (2) *Suppose that $R \searrow_w N$ and that $(s, R) \xrightarrow{a} (s', M')$ for some a not in $\text{Ran}(w) \setminus \text{Ran}(w_p)$. Then we have $w \models (s_w, N) \xrightarrow{a} (s'_w, N')$ for some N' with $M' \searrow_w N'$.*

The third lemma concerns evaluation contexts. The simulation relation is again extended in the evident way to evaluation contexts, taking $[-] \searrow_w [-]$, etc. One easily sees that if $E \searrow_w E'$ and $M \searrow_w N$ then $E[M] \searrow_w E'[N]$.

LEMMA B.9. *Suppose that $E[R] \searrow_w N$. Then N has the form $E'[N_1]$ where $E \searrow_w E'$ and $R \searrow_w N_1$.*

Using these results, one obtains a small-step simulation lemma, Lemma 5.3, which, in its turn, yields Proposition 5.4, the big-step simulation result.

B.4. High- and Low-Level Attackers

PROOF OF THEOREM 5.7. Fix M, C , and s . The proof proceeds by cases on whether or not $|\text{Acc}(CM, s)| \leq b$. Suppose first that $|\text{Acc}(CM, s)| \leq b$. Take a w such that $w \# \text{Acc}(CM, s)$. Then, by Proposition 5.4, $\text{Acc}(CM, s) = \text{Acc}_w(CM^\downarrow, s_w)$ and $\text{Eval}(CM, s)_w = \text{Eval}_w(CM^\downarrow, s_w)$, as $CM \searrow_w (CM)^\downarrow = CM^\downarrow$. By Proposition 5.1, we also have that $\text{Eval}(C^\uparrow M, s) = \text{Eval}(CM, s)$.

We therefore have:

$$\begin{aligned} \delta_b &\leq \delta_{|\text{Acc}(CM, s)|} \\ &\leq P(w \# \text{Acc}(CM, s)) \\ &\leq P(|\text{Acc}_w(CM^\downarrow, s_w)| \leq b \text{ and } \text{Eval}(C^\uparrow M, s)_w = \text{Eval}_w(CM^\downarrow, s_w)) \end{aligned}$$

which is the second alternative.

Otherwise, we have $|\text{Acc}(CM, s)| > b$. So, as $(s, CM) \xrightarrow{A} (s', M')$ for some s', M' , and A with $\text{Acc}(CM, s) = A \cap \{0, \dots, c\}$, we have $(s, CM) \xrightarrow{A'} (s'', M'')$ for some s'', M'' , and A' , where, setting $A'' = A' \cap \{0, \dots, c\}$, $|A''| = b + 1$.

Now, take a w such that $w \# A''$. Then, as $CM \searrow_w CM^\downarrow$, Lemma 5.3 implies that $w \models (s_w, CM^\downarrow) \xrightarrow{A'} (s''_w, N)$, for some N , and so $\text{Acc}_w(CM^\downarrow, s_w) \supseteq A''$ and $|\text{Acc}_w(CM^\downarrow, s_w)| > b$. We therefore have:

$$\begin{aligned} \delta_{b+1} &\leq P(w \# A'') \\ &\leq P(|\text{Acc}_w(CM^\downarrow, s_w)| > b) \end{aligned}$$

which is the first alternative. $\square$

B.5. Equivalences

PROOF OF THEOREM 5.8. In one direction, we assume that $M \approx_{h,p} N$, and then consider a public low-level term $C : \sigma \rightarrow \text{bool}$ in order to show that $CM^\downarrow \sim_{l,p}^b CN^\downarrow$. Choose a store s . Applying Theorem 5.7 to M and N , four cases arise.

(1) In the first case, we have:

$$P(|\text{Acc}_w(CM^\downarrow, s_w)| > b) \geq \delta_{b+1} \quad \text{and} \quad P(|\text{Acc}_w(CN^\downarrow, s_w)| > b) \geq \delta_{b+1}$$

But then

$$P(\text{Eval}_w^b(CM^\downarrow, s_w) = \Omega) \geq \delta_{b+1} \quad \text{and} \quad P(\text{Eval}_w^b(CN^\downarrow, s_w) = \Omega) \geq \delta_{b+1}$$

concluding this case.

(2) In the second case, we have:

$$P\left(\begin{array}{l} |\text{Acc}_w(CM^\downarrow, s_w)| \leq b \quad \text{and} \\ \text{Eval}(C^\uparrow M, s)_w = \text{Eval}_w(CM^\downarrow, s_w) \end{array}\right) \geq \delta_b.$$

and

$$P\left(\begin{array}{l} |\text{Acc}_w(CN^\downarrow, s_w)| \leq b \quad \text{and} \\ \text{Eval}(C^\uparrow N, s)_w = \text{Eval}_w(CN^\downarrow, s_w) \end{array}\right) \geq \delta_b.$$

By assumption, we have $\text{Eval}(C^\dagger M, s) =_p \text{Eval}(C^\dagger N, s)$ so there are two subcases.

(a) In the first, there are s', s'' , and V such that $s' \upharpoonright \text{PubLoc} = s'' \upharpoonright \text{PubLoc}$, $\text{Eval}(C^\dagger M, s) = (s', V)$, and $\text{Eval}(C^\dagger N, s) = (s'', V)$. But then we have:

$$\text{P}(\text{Eval}_w^b(CM^\downarrow, s_w) = (s'_w, V)) \geq \delta_b \quad \text{and} \quad \text{P}(\text{Eval}_w^b(CN^\downarrow, s_w) = (s''_w, V)) \geq \delta_b$$

concluding this subcase.

(b) In the second, $\text{Eval}(C^\dagger M, s) = \text{Eval}(C^\dagger N, s) = \Omega$, and we obtain:

$$\text{P}(\text{Eval}_w^b(CM^\downarrow, s_w) = \Omega) \geq \delta_b \quad \text{and} \quad \text{P}(\text{Eval}_w^b(CN^\downarrow, s_w) = \Omega) \geq \delta_b$$

concluding this subcase.

(3) In the third case, we have:

$$\text{P}(|\text{Acc}_w(CM^\downarrow, s_w)| > b) \geq \delta_{b+1}$$

and

$$\text{P} \left(\begin{array}{l} |\text{Acc}_w(CN^\downarrow, s_w)| \leq b \quad \text{and} \\ \text{Eval}(C^\dagger N, s)_w = \text{Eval}_w(CN^\downarrow, s_w) \end{array} \right) \geq \delta_b$$

There are again two subcases.

(a) In the first, $\text{Eval}(C^\dagger N, s)$ has the form (s', V) for some s' and V . So we have $(s, CN) \xrightarrow{A'} (s', V)$ for some A' with $A' \cap \{0, \dots, c\} = \text{Acc}(CN, s)$, as otherwise (i.e., if $(s, CN) \uparrow^{A'}$, for some A'), by Proposition 5.1 we would have a contradiction with the form of $\text{Eval}(C^\dagger N, s)$.

By the remark after Theorem 5.7, and since the alternatives there are mutually exclusive, we have, using the assumptions of this case, that $|\text{Acc}(CM, s)| > b$; we similarly have that $|\text{Acc}(CN, s)| \leq b$. So $\text{Acc}(CM, s) \setminus \text{Acc}(CN, s)$ is non-empty, and we choose an element a of it; note that $a \notin \text{Ran}(w_p)$.

We know that $(s, CN) \xrightarrow{A'} (s', V)$. So, as $(CN)_a^\dagger = C_a^\dagger N$, by Proposition 5.2 we have $(s, C_a^\dagger N) \Rightarrow (s', V)$. However, we have $(s, C_a^\dagger M) \uparrow$ by parts 3 and 4 of Proposition 5.2. This contradicts the assumption that $M \approx_{h,p} N$.

(b) In the second, $\text{Eval}(C^\dagger N, s) = \Omega$. But then we have

$$\text{P}(\text{Eval}_w^b(CM^\downarrow, s_w) = \Omega) \geq \delta_{b+1} \quad \text{and} \quad \text{P}(\text{Eval}_w^b(CN^\downarrow, s_w) = \Omega) \geq \delta_b \geq \delta_{b+1}$$

concluding this subcase.

(1) The fourth case, is similar to the third.

In the other direction, assume that $M^\downarrow \approx_{l,p}^b N^\downarrow$ and then consider a public high-level term $C : \sigma \rightarrow \text{bool}$ in order to show, for a given store s , that $\text{Eval}(CM, s) =_p \text{Eval}(CN, s)$. We know that $C^\downarrow M^\downarrow \sim_{l,p}^b C^\downarrow N^\downarrow$. For any w we also know by Proposition 5.5 that $\text{Acc}_w(C^\downarrow M^\downarrow, s_w) = \emptyset$, so, by Corollary 5.6 and the definition of Eval_w^b , that

$$\text{Eval}(CM, s)_w = \text{Eval}_w(C^\downarrow M^\downarrow, s_w) = \text{Eval}_w^b(C^\downarrow M^\downarrow, s_w)$$

The same holds for N .

The definition of $\sim_{l,p}^b$ then yields two cases.

(1) In the first case, we have:

$$\text{P}(\text{Eval}_w^b(C^\downarrow M^\downarrow, s_w) = (s'_w, V)) \geq \delta_b$$

and

$$\text{P}(\text{Eval}_w^b(C^\downarrow N^\downarrow, s_w) = (s''_w, V)) \geq \delta_b$$

for some $s' \upharpoonright \text{PubLoc} = s'' \upharpoonright \text{PubLoc}$ and V . As $\delta_b > 0$, $\text{Eval}_{w'}^b(C^\downarrow M^\downarrow, s_{w'}) = (s'_{w'}, V)$ and $\text{Eval}_{w''}^b(C^\downarrow N^\downarrow, s_{w''}) = (s''_{w''}, V)$, for some w' and w'' . So,

$$\text{Eval}(CM, s)_{w'} = \text{Eval}_{w'}^b(C^\downarrow M^\downarrow, s_{w'}) = (s'_{w'}, V)$$

and

$$\text{Eval}(CN, s)_{w''} = \text{Eval}_{w''}^b(C^\downarrow N^\downarrow, s_{w''}) = (s''_{w''}, V)$$

As the map $s \mapsto s_w$ is injective, $\text{Eval}(CM, s) = (s', V)$ and $\text{Eval}(CN, s) = (s'', V)$. Therefore, $\text{Eval}(CM, s) =_p \text{Eval}(CN, s)$, concluding this case.

(2) In the second case, we have:

$$P(\text{Eval}_w^b(C^\downarrow M^\downarrow, s_w) = \Omega) \geq \delta_{b+1} \quad \text{and} \quad P(\text{Eval}_w^b(C^\downarrow N^\downarrow, s_w) = \Omega) \geq \delta_{b+1}$$

As $\delta_{b+1} > 0$ there are w' and w'' such that

$$\text{Eval}_{w'}(C^\downarrow M^\downarrow, s_{w'}) = \text{Eval}_{w''}(C^\downarrow N^\downarrow, s_{w''}) = \Omega$$

So $\text{Eval}(CM, s) = \text{Eval}(CN, s) = \Omega$ concluding the proof. $\square$