Equational Properties of Mobile Ambients

Andrew D. Gordon
Microsoft Research

Luca Cardelli
Microsoft Research

April 1999

Technical Report
MSR-TR-99-11

Microsoft Research
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

A shortened version of this paper appears in the proceedings of the conference on *Foundations of Software Science and Computation Structures*, Amsterdam, the Netherlands, 22–26 March 1999. The proceedings is published by Springer Verlag as a volume of the series *Lecture Notes in Computer Science.*

Equational Properties of Mobile Ambients

Andrew D. Gordon
Microsoft Research

Luca Cardelli
Microsoft Research

April 1999

Abstract

The ambient calculus is a process calculus for describing mobile computation. We develop a theory of Morris-style contextual equivalence for proving properties of mobile ambients. We prove a context lemma that allows derivation of contextual equivalences by considering contexts of a particular limited form, rather than all arbitrary contexts. We give an activity lemma that characterizes the possible interactions between a process and a context. We prove several examples of contextual equivalence. The proofs depend on characterizing reductions in the ambient calculus in terms of a labelled transition system.

Contents

1 Motivation

This paper develops tools for proving equations in the ambient calculus.

In earlier work [7], we introduced the ambient calculus by adding *ambients*—mobile, hierarchical protection domains—to a framework for concurrency extracted from the π-calculus [13]. The ambient calculus is an abstract model of mobile computation, including both mobile software agents and mobile hardware devices. The calculus models access control as well as mobility. For example, a process may move into or out of a particular ambient only if it possesses the appropriate capability.

This paper focuses on behavioural equivalence of mobile ambients. In particular, we study a form of Morris' contextual equivalence [15] for ambients and develop some proof techniques. Our motivation is to prove a variety of equations. Some of these equations express and confirm some of the informal principles we had in mind when designing the calculus. As in other recent work [1, 2], some of the equations establish security properties of systems modelled within the calculus.

The inclusion of primitives for mobility makes the theory of the ambient calculus more complex than that of its ancestor, the π-calculus. The main contribution of this paper is to demonstrate that some standard tools—a labelled transition system, a context lemma, and an activity lemma—may be recast in the setting of the ambient calculus. Moreover, the paper introduces a new technique—based on what we call the hardening relation—for factoring the definition of the labelled transition system into a set of rules that identify the individual processes participating in a transition, and a set of rules that express how the participant processes interact.

We begin, in Section 2, by reviewing the syntax and reduction semantics of the ambient calculus. The semantics consists of a structural congruence relation $P \equiv Q$ (which says that P may be structurally rearranged to yield Q) and a reduction relation $P \rightarrow Q$ (which says that P may evolve in one step of computation to yield Q).

We introduce contextual equivalence $P \simeq Q$ in Section 3. We define a predicate, $P \Downarrow n$, which means intuitively that an observer may eventually detect an ambient named n at the top-level of the process P. Then we define $P \simeq Q$ to mean that, whenever P and Q are placed within an arbitrary context constructed from the syntax of the calculus, any observation made of P may also be made of Q, and vice versa. We give examples of pairs of processes that are equivalent and examples of pairs that are inequivalent.

In Section 4, we describe some techniques for proving contextual equivalence. We introduce a second operational semantics for the ambient calculus based on a hardening relation and a labelled transition system. The hardening relation identifies the subprocesses of a process that may participate in a computation step. We use the hardening relation both for defining the labelled transition system and for characterizing whether an ambient of a particular name is present at the top-level of a process. Our first result, Theorem 9, asserts that the τ-labelled transition relation and the reduction relation are the same, up to structural congruence. So our two operational semantics are equivalent. The labelled transition system is useful for analyzing the possible evolution of a process, since we may read off the possible labelled transitions of a process by inspecting its syntactic structure. Our second result, Theorem 12 is a context lemma that allows us to prove contextual equivalence by considering a limited set of contexts, known as harnesses, rather than all arbitrary contexts. A harness is a context with a single hole that is enclosed only within parallel compositions, restrictions, and ambients. The third result of this section, Theorem 15, is an activity lemma that elaborates the ways in which a reduction may be derived when a process is inserted into a harness: either the process reduces by itself, or the harness reduces by itself, or there is an interaction between the harness and the process.

We exercise these proof techniques on examples in Section 5, and conclude in Section 6. Appendix A contains proofs omitted from the main body of the paper.

2 The Ambient Calculus (Review)

We briefly describe the syntax and semantics of the calculus. We assume there are infinite sets of *names* and *variables*, ranged over by m, n, p, q, and x, y, z, respectively. The syntax of the ambient calculus is based on categories of *expressions* and *processes*, ranged over by M, N, and P, Q, R, respectively. The calculus inherits a core of concurrency primitives from the π-calculus: a restriction $(\nu n)P$ creates a fresh name n whose scope is P; a composition $P \mid Q$ behaves as P and Q running in parallel; a replication $!P$ behaves as unboundedly many replicas of P running in parallel; and the inactive process $\mathbf{0}$ does nothing. We augment these π-calculus processes with primitives for mobility—ambients, $n[P]$, and the exercise of capabilities, $M.P$—and primitives for communication—input, $(x).P$, and output, $\langle M \rangle$.

Here is an example process that illustrates the new primitives for mobility and communication:

$$m[p[\mathit{out}\, m.\mathit{in}\, n.\langle M \rangle]] \mid n[\mathit{open}\, p.(x).Q]$$

The effect of the mobility primitives in this example is to move the ambient p out of m and into n, and then to open it up. The input $(x).Q$ may then consume the output $\langle M \rangle$ to leave the residue $m[] \mid n[Q\{x{\leftarrow}M\}]$. We may regard the ambients m and n in this example as modelling two machines on a network, and the ambient p as modelling a packet sent from m to n. Next, we describe the semantics of the new primitives in more detail.

An ambient $n[P]$ is a boundary, named n, around the process P. The boundary prevents direct interactions between P and any processes running in parallel with $n[P]$, but it does not prevent interactions within P. Ambients may be nested, so they induce a hierarchy. For example, in the process displayed above, the ambient named m is a parent of the ambient named p, and the ambients named m and n are siblings.

An action $M.P$ exercises the capabilities represented by M, and then behaves as P. The action either affects an enclosing ambient or one running in parallel. A capability is an expression derived from the name of an ambient. The three basic capabilities are *in* n, *out* n, and *open* n. An action *in* $n.P$ moves its enclosing ambient into a sibling ambient named n. An action *out* $n.P$ moves its enclosing ambient out of its parent ambient, named n, to become a sibling of the former parent. An action *open* $n.P$ dissolves the boundary of an ambient $n[Q]$ running in parallel; the outcome is that the residue P of the action and the residue Q of the opened ambient run in parallel. In general, the expression M in $M.P$ may stand for a finite sequence of the basic capabilities, which are exercised one by one. Finite sequences are built up using concatenation, written $M.M'$. The empty sequence is written ϵ.

The final two process primitives allow communication of expressions. Expressions include names, variables, and capabilities. An output $\langle M \rangle$ outputs the expression M. An input $(x).P$ blocks until it may consume an output running in parallel. Then it binds the expression being output to the variable x, and runs P. In $(x).P$, the variable x is bound; its scope is P. Inputs and outputs are local to the enclosing ambient. Inputs and outputs may not interact directly through an ambient boundary. Hence we may think of there being an implicit input/output channel associated with each ambient.

We formally specify the syntax of the calculus as follows:

Expressions and Processes:

$M, N ::=$	expressions	$P, Q, R ::=$	processes
x	variable	$(\nu n)P$	restriction
n	name	$\mathbf{0}$	inactivity
in M	can enter M	$P \mid Q$	composition
out M	can exit M	$!P$	replication
open M	can open M	$M[P]$	ambient
ϵ	null	$M.P$	action
$M.M'$	path	$(x).P$	input
		$\langle M \rangle$	output

In situations where a process is expected, we often write just M as a shorthand for the process $M.\mathbf{0}$. We often write just $M[]$ as a shorthand for the process $M[\mathbf{0}]$. We write $(\nu\vec{p})P$ as a shorthand for $(\nu p_1) \cdots (\nu p_k)P$ where $\vec{p} = p_1, \ldots, p_k$.

We let $fn(M)$ and $fv(M)$ be the sets of *free names* and *free variables*, respectively, of an expression M. Similarly, $fn(P)$ and $fv(P)$ are the sets of *free names* and *free variables* of a process P. If a phrase ϕ is an expression or a process, we write $\phi\{x \leftarrow M\}$ and $\phi\{n \leftarrow M\}$ for the outcomes of capture-avoiding substitutions of the expression M for each free occurrence of the variable x and the name n, respectively, in ϕ. We identify processes up to consistent renaming of bound names and variables.

We formally define the operational semantics of ambient calculus in the chemical style, using structural congruence and reduction relations:

Structural Congruence: $P \equiv Q$

$$
\begin{array}{ll}
P \mid Q \equiv Q \mid P & P \equiv P \\
(P \mid Q) \mid R \equiv P \mid (Q \mid R) & Q \equiv P \Rightarrow P \equiv Q \\
!P \equiv P \mid !P & P \equiv Q, Q \equiv R \Rightarrow P \equiv R \\
(\nu n)(\nu m)P \equiv (\nu m)(\nu n)P & \\
n \notin \mathit{fn}(P) \Rightarrow (\nu n)(P \mid Q) \equiv P \mid (\nu n)Q & P \equiv Q \Rightarrow (\nu n)P \equiv (\nu n)Q \\
n \neq m \Rightarrow (\nu n)m[P] \equiv m[(\nu n)P] & P \equiv Q \Rightarrow P \mid R \equiv Q \mid R \\
P \mid \mathbf{0} \equiv P & P \equiv Q \Rightarrow !P \equiv !Q \\
(\nu n)\mathbf{0} \equiv \mathbf{0} & P \equiv Q \Rightarrow M[P] \equiv M[Q] \\
!\mathbf{0} \equiv \mathbf{0} & P \equiv Q \Rightarrow M.P \equiv M.Q \\
\epsilon.P \equiv P & P \equiv Q \Rightarrow (x).P \equiv (x).Q \\
(M.M').P \equiv M.M'.P &
\end{array}
$$

Reduction: $P \rightarrow Q$

$$
\begin{array}{ll}
n[\mathit{in}\, m.P \mid Q] \mid m[R] \rightarrow m[n[P \mid Q] \mid R] & P \rightarrow Q \Rightarrow P \mid R \rightarrow Q \mid R \\
m[n[\mathit{out}\, m.P \mid Q] \mid R] \rightarrow n[P \mid Q] \mid m[R] & P \rightarrow Q \Rightarrow (\nu n)P \rightarrow (\nu n)Q \\
\mathit{open}\, n.P \mid n[Q] \rightarrow P \mid Q & P \rightarrow Q \Rightarrow n[P] \rightarrow n[Q] \\
\langle M \rangle \mid (x).P \rightarrow P\{x \leftarrow M\} & P' \equiv P, P \rightarrow Q, Q \equiv Q' \Rightarrow P' \rightarrow Q'
\end{array}
$$

For example, the process displayed earlier has the following reductions:

$$
\begin{array}{rcl}
m[p[\mathit{out}\, m.\mathit{in}\, n.\langle M \rangle]] \mid n[\mathit{open}\, p.(x).P] & \rightarrow & m[] \mid p[\mathit{in}\, n.\langle M \rangle] \mid n[\mathit{open}\, p.(x).P] \\
& \rightarrow & m[] \mid n[p[\langle M \rangle] \mid \mathit{open}\, p.(x).P] \\
& \rightarrow & m[] \mid n[\langle M \rangle \mid (x).P] \\
& \rightarrow & m[] \mid n[P\{x \leftarrow M\}]
\end{array}
$$

The syntax allows the formation of certain processes that may not participate in any reductions, such as the action $n.P$ and the ambient $(\mathit{in}\ n)[P]$. The presence of these nonsensical processes is harmless as far as the purposes of this paper are concerned. They may be ruled out by a simple type system [8].

This concludes our brief review of the calculus. Earlier papers [6, 7] explain in detail the motivation for our calculus, and give programming examples.

3 Contextual Equivalence

Morris-style contextual equivalence [15] (otherwise known as may-testing equivalence [9]) is a standard way of saying that two processes have the same behaviour: two processes are contextually equivalent if and only if they admit the same elementary observations whenever they are inserted inside any arbitrary enclosing process. In the setting of the ambient calculus, we shall define contextual equivalence in terms of observing the presence, at the top-level of a process, of an ambient whose name is not restricted.

Let us say that a process P *exhibits a name* n just if P is a process with a top-level ambient named n, that is not restricted:

Exhibition of a Name: $P \downarrow n$

$$P \downarrow n \quad \triangleq \quad \text{there are } \vec{m}, P', P'' \text{ with } n \notin \{\vec{m}\} \text{ and } P \equiv (\nu\vec{m})(n[P'] \mid P'')$$

Let us say that a process P *converges to a name* n just if after some number of reductions, P exhibits n:

Convergence to a Name: $P \Downarrow n$

(Conv Exh) (Conv Red)

$$\frac{P \downarrow n}{P \Downarrow n} \qquad \frac{P \rightarrow Q \qquad Q \Downarrow n}{P \Downarrow n}$$

Next, let a *context*, $\mathcal{C}()$, be a process containing zero or more holes. We write a hole as $()$. We write $\mathcal{C}(P)$ for the outcome of filling each of the holes in the context $\mathcal{C}$ with the process P. Variables and names free in P may become bound in $\mathcal{C}(P)$. For example, if $P = n[\langle x\rangle]$ and $\mathcal{C}() = (\nu n)(x).()$, the variable x and the name n have become bound in $\mathcal{C}(P) = (\nu n)(x).n[\langle x\rangle]$. Hence, we do not identify contexts up to renaming of bound variables and names.

Now, we can formally define contextual equivalence of processes:

Contextual Equivalence: $P \simeq Q$

$$P \simeq Q \quad \triangleq \quad \text{for all } n, \mathcal{C}() \text{ with } \mathcal{C}(P), \mathcal{C}(Q) \text{ closed, } \mathcal{C}(P) \Downarrow n \Leftrightarrow \mathcal{C}(Q) \Downarrow n$$

The following two propositions state some basic properties enjoyed by contextual equivalence. Let a relation $\mathcal{R}$ be a *precongruence* if and only if, for all P, Q, and $\mathcal{C}()$, if $P \mathrel{\mathcal{R}} Q$ then $\mathcal{C}(P) \mathrel{\mathcal{R}} \mathcal{C}(Q)$. If, in addition, $\mathcal{R}$ is reflexive, symmetric, and transitive, we say it is a *congruence*. For example, the structural congruence relation has these properties. Moreover, by a standard argument, so has contextual equivalence:

Proposition 1 *Contextual equivalence is a congruence.*

Structural congruence preserves exhibition of or convergence to a name, and hence is included in contextual equivalence:

Lemma 2 *Suppose $P \equiv Q$. If $P \downarrow n$ then $Q \downarrow n$. Moreover, if $P \Downarrow n$ then $Q \Downarrow n$ with the same depth of inference.*

Proof For part (1), $P \downarrow n$, by definition, means that there are $\vec{m}$, P', P'' with $n \notin \{\vec{m}\}$ and $P \equiv (\nu\vec{m})(n[P'] \mid P'')$. Since $P \equiv Q$, we have $Q \equiv (\nu\vec{m})(n[P'] \mid P'')$, and hence $Q \downarrow n$. Part (2) follows by a case analysis of the derivation of $P \Downarrow n$. □

Proposition 3 *If $P \equiv Q$ then $P \simeq Q$.*

Proof Consider any context $\mathcal{C}()$ and any name n, such that $\mathcal{C}(P) \Downarrow n$. Since $\equiv$ is a congruence, $P \equiv Q$ implies $\mathcal{C}(P) \equiv \mathcal{C}(Q)$. By Lemma 2, this and $\mathcal{C}(P) \Downarrow n$ imply $\mathcal{C}(Q) \Downarrow n$. Similarly, we can show that for all $\mathcal{C}$ and n, $\mathcal{C}(Q) \Downarrow n$ implies $\mathcal{C}(P) \Downarrow n$. Hence $P \simeq Q$. □

The following two examples illustrate that to show that two processes are contextually inequivalent, it suffices to find a context that distinguishes them.

Example 1 *If* $m \neq n$ *then* $m[] \not\simeq n[]$.

Proof Consider the context $\mathcal{C}() = ()$. Since $\mathcal{C}(m[]) \equiv m[]$, we have $\mathcal{C}(m[]) \downarrow m$. By (Conv Exh), $\mathcal{C}(m[]) \Downarrow m$. On the other hand, the process $n[]$ has no reductions, and does not exhibit m. Hence, we cannot derive $\mathcal{C}(n[]) \Downarrow m$. □

Example 2 *If* $m \neq n$ *then* $\mathit{open}\, m.\mathbf{0} \not\simeq \mathit{open}\, n.\mathbf{0}$.

Proof Let $\mathcal{C}() = m[p[]] \mid ()$. Then $\mathcal{C}(\mathit{open} m.\mathbf{0}) \Downarrow p$ but not $\mathcal{C}(\mathit{open} n.\mathbf{0}) \Downarrow p$.□

On the other hand, it is harder to show that two processes are contextually equivalent, since one must consider their behaviour when placed in an arbitrary context. For example, consider the following contextual equivalence:

Example 3 $(\nu n)(n[] \mid \mathit{open}\, n.P) \simeq P$ *if* $n \notin \mathit{fn}(P)$.

The restriction of the name n in the process $(\nu n)(n[] \mid \mathit{open} n.P)$ implies that no context may interact with this process until it has reduced to P. Therefore, we would expect the equation to hold. But to prove this and other equations formally we need some further techniques, which we develop in the next section. We return to Example 3 in Section 5.

4 Tools for Proving Contextual Equivalence

The tools we introduce are relations and theorems that help prove contextual equivalence.

4.1 A Hardening Relation

In this section, we define a relation that explicitly identifies the top-level subprocesses of a process that may be involved in a reduction. This relation, the *hardening* relation, takes the form, $P > (\nu p_1, \ldots, p_k)\langle P' \rangle P''$, where the phrase $(\nu p_1, \ldots, p_k)\langle P' \rangle P''$ is called a *concretion.* We say that P' is the *prime* of the concretion, and that P'' is the *residue* of concretion. Both P' and P'' lie in the scope of the restricted names $p_1, \ldots, p_k$. The intuition is that the process P, which may have many top-level subprocesses, may harden to a concretion that singles out a prime subprocess P', leaving behind the residue P''. By saying that P' has a top-level occurrence in P, we mean that P' is a subprocess of P not enclosed within any ambient boundaries. In the next section, we use the hardening relation to define an operational semantics for the ambient calculus in terms of interactions between top-level occurrences of processes.

Concretions were introduced by Milner in the context of the π-calculus [11]. For the ambient calculus, we specify them as follows, where the prime of the concretion must be an action, an ambient, an input, or an output:

Concretions:

$C, D ::=$	concretions
$(\nu\vec{p})\langle M.P\rangle Q$	action, $M \in \{\mathit{in}\, n, \mathit{out}\, n, \mathit{open}\, n\}$
$(\nu\vec{p})\langle n[P]\rangle Q$	ambient
$(\nu\vec{p})\langle (x).P\rangle Q$	input
$(\nu\vec{p})\langle\langle M\rangle\rangle Q$	output

The order of the bound names $p_1, \ldots, p_k$ in a concretion $(\nu p_1, \ldots, p_k)\langle P'\rangle P''$ does not matter and they may be renamed consistently. When $k = 0$, we may write the concretion as $(\nu)\langle P'\rangle P''$.

We now introduce the basic ideas of the hardening relation informally. If P is an action $\mathit{in}\, n.Q$, $\mathit{out}\, n.Q$, $\mathit{open}\, n.Q$, an ambient $n[Q]$, an input $(x).Q$, or an output $\langle M\rangle$, then P hardens to $(\nu)\langle P\rangle\mathbf{0}$. Consider two processes P and Q. If either of these hardens to a concretion, then their composition $P \mid Q$ may harden to the same concretion, but with the other process included in the residue of the concretion. For example, if $P > (\nu)\langle P_1\rangle P_2$ then $P \mid Q > (\nu)\langle P_1\rangle(P_2 \mid Q)$. If a process P hardens to a concretion, then the replication $!P$ may harden to the same concretion, but with $!P$ included in the residue of the concretion—a replication is not consumed by hardening. Finally, if a process P hardens to a concretion C, then the restriction $(\nu n)P$ hardens to a concretion written $\overline{(\nu n)}C$, which is the same as C but with the restriction (νn) included either in the list of bound names, the prime, or the residue of C. We define $\overline{(\nu n)}C$ by:

Restricting a Concretion: $\overline{(\nu n)}C$ where $C = (\nu\vec{p})\langle P_1\rangle P_2$ and $n \notin \{\vec{p}\}$

(1) If $n \in \mathit{fn}(P_1)$ then:

(a) If $P_1 = m[P_1']$, $m \neq n$, $n \notin \mathit{fn}(P_2)$, let $\overline{(\nu n)}C \triangleq (\nu\vec{p})\langle m[(\nu n)P_1']\rangle P_2$.

(b) Otherwise, let $\overline{(\nu n)}C \triangleq (\nu n, \vec{p})\langle P_1\rangle P_2$.

(2) If $n \notin \mathit{fn}(P_1)$ let $\overline{(\nu n)}C \triangleq (\nu\vec{p})\langle P_1\rangle(\nu n)P_2$.

Next, we define the hardening relation by the following:

Hardening: $P > C$

(Harden Action) (Harden ϵ) (Harden .)

$$\frac{M \in \{\mathit{in}\, n, \mathit{out}\, n, \mathit{open}\, n\}}{M.P > (\nu)\langle M.P\rangle\mathbf{0}} \qquad \frac{P > C}{\epsilon.P > C} \qquad \frac{M.(N.P) > C}{(M.N).P > C}$$

(Harden Amb) (Harden Input) (Harden Output)

$$\frac{}{n[P] > (\nu)\langle n[P]\rangle\mathbf{0}} \qquad \frac{}{(x).P > (\nu)\langle(x).P\rangle\mathbf{0}} \qquad \frac{}{\langle M\rangle > (\nu)\langle\langle M\rangle\rangle\mathbf{0}}$$

(Harden Par 1) (for $\{\vec{p}\} \cap \mathit{fn}(Q) = \varnothing$)

$$\frac{P > (\nu\vec{p})\langle P'\rangle P''}{P \mid Q > (\nu\vec{p})\langle P'\rangle(P'' \mid Q)}$$

(Harden Par 2) (for $\{\vec{q}\} \cap \mathit{fn}(P) = \varnothing$)

$$\frac{Q > (\nu\vec{q})\langle Q'\rangle Q''}{P \mid Q > (\nu\vec{q})\langle Q'\rangle(P \mid Q'')}$$

(Harden Repl)

$$\frac{P > (\nu\vec{p})\langle P'\rangle P''}{!P > (\nu\vec{p})\langle P'\rangle(P'' \mid !P)}$$

(Harden Res)

$$\frac{P > C}{(\nu n)P > \overline{(\nu n)}C}$$

For example, the process $P = (\nu p)(\nu q)(n[p[]] \mid q[])$ may harden in two ways:

$$\begin{array}{lcl} P & > & (\nu)\langle n[(\nu p)p[]]\rangle(\nu q)(\mathbf{0} \mid q[]) \\ P & > & (\nu q)\langle q[]\rangle(\nu p)(n[p[]] \mid \mathbf{0}) \end{array}$$

The following is a basic property of hardening:

Lemma 4 *If $P > (\nu\vec{p})\langle P'\rangle P''$ then $\{\vec{p}\} \subseteq \mathit{fn}(P')$ and the names $\vec{p}$ are pairwise distinct.*

Proof By induction on the derivation of $P > (\nu\vec{p})\langle P'\rangle P''$. □

The next two results relate hardening and structural congruence.

Lemma 5 *If $P > (\nu\vec{p})\langle P'\rangle P''$ then $P \equiv (\nu\vec{p})(P' \mid P'')$.*

Proposition 6 *If $P \equiv Q$ and $Q > (\nu\vec{r})\langle Q'\rangle Q''$ then there are P' and P'' with $P > (\nu\vec{r})\langle P'\rangle P''$, $P' \equiv Q'$, and $P'' \equiv Q''$.*

These results follow from inductions on the derivations of $P > (\nu\vec{p})\langle P'\rangle P''$ and $P \equiv Q$, respectively. Using them, we may characterize exhibition of a name independently of structural congruence:

Proposition 7 *$P \downarrow n$ if and only if there are $\vec{p}$, P', P'', such that $P > (\nu\vec{p})\langle n[P']\rangle P''$ and $n \notin \{\vec{p}\}$.*

Now, we can show that the hardening relation is image-finite:

Lemma 8 *For all P, $\{C : P > C\}$ is finite.*

Proof By induction on the structure of P. □

The proof suggests a procedure for the enumerating the set $\{C : P > C\}$. Given Proposition 7, it follows that the predicate $P \downarrow n$ is decidable.

4.2 A Labelled Transition System

The labelled transition system presented in this section allows for an analysis of the possible reductions from a process P in terms of the syntactic structure of P. The definition of the reduction relation does not directly support such an analysis, because of the rule $P' \equiv P, P \rightarrow Q, Q \equiv Q' \Rightarrow P' \rightarrow Q'$, which allows for arbitrary structural rearrangements of a process during the derivation of a reduction.

We define a family of transition relations $P \xrightarrow{\alpha} Q$, indexed by a set of labels, ranged over by α, which is given in the following table:

Labels:

$\alpha ::=$	label
τ	internal step
$in\, n$	enter ambient n
$out\, n$	exit ambient n
$open\, n$	dissolve ambient n

An M-transition $P \xrightarrow{M} Q$ means that the process P has a top-level process exercising the capability M; these transitions are defined by the rule (Trans Cap) below. A τ-transition $P \xrightarrow{\tau} Q$ means that P evolves in one step to Q; these transitions are defined by the other rules below.

Labelled Transitions: $P \xrightarrow{\alpha} P'$

(Trans Cap)

$$\frac{P > (\nu\vec{p})\langle M.P'\rangle P'' \quad fn(M) \cap \{\vec{p}\} = \varnothing}{P \xrightarrow{M} (\nu\vec{p})(P' \mid P'')}$$

(Trans Amb)

$$\frac{P > (\nu\vec{p})\langle n[Q]\rangle P' \quad Q \xrightarrow{\tau} Q'}{P \xrightarrow{\tau} (\nu\vec{p})(n[Q'] \mid P')}$$

(Trans In) (where $\{\vec{r}\} \cap fn(n[Q]) = \varnothing$ and $\{\vec{r}\} \cap \{\vec{p}\} = \varnothing$)

$$\frac{P > (\nu\vec{p})\langle n[Q]\rangle R \quad Q \xrightarrow{in\, m} Q' \quad R > (\nu\vec{r})\langle m[R']\rangle R''}{P \xrightarrow{\tau} (\nu\vec{p},\vec{r})(m[n[Q'] \mid R'] \mid R'')}$$

(Trans Out) (where $n \notin \{\vec{q}\}$)

$$\frac{P > (\nu\vec{p})\langle n[Q]\rangle P' \quad Q > (\nu\vec{q})\langle m[R]\rangle Q' \quad R \xrightarrow{out\, n} R'}{P \xrightarrow{\tau} (\nu\vec{p})((\nu\vec{q})(m[R'] \mid n[Q']) \mid P')}$$

(Trans Open)

$$\frac{P > (\nu\vec{p})\langle n[Q]\rangle P' \quad P' \xrightarrow{open\, n} P''}{P \xrightarrow{\tau} (\nu\vec{p})(Q \mid P'')}$$

(Trans I/O) (where $\{\vec{q}\} \cap fn(\langle M \rangle) = \varnothing$)

$$\frac{P > (\nu\vec{p})\langle\langle M\rangle\rangle P' \quad P' > (\nu\vec{q})\langle(x).P''\rangle P'''}{P \xrightarrow{\tau} (\nu\vec{p},\vec{q})(P''\{x{\leftarrow}M\} \mid P''')}$$

The rules (Trans In), (Trans Out), and (Trans Open) derive a τ-transition from an M-transition. We introduced the M-transitions to simplify the statement of these three rules. (Trans I/O) allows for exchange of messages. (Trans Amb) is a congruence rule for τ-transitions within ambients.

Given its definition in terms of the hardening relation, we may analyze the transitions derivable from any process by inspection of its syntactic structure. This allows a structural analysis of the possible reductions from a process, since the τ-transition relation corresponds to the reduction relation as in the following theorem, where $P \xrightarrow{\tau}\equiv Q$ means there is R with $P \xrightarrow{\tau} R$ and $R \equiv Q$.

Theorem 9 *$P \to Q$ if and only if $P \xrightarrow{\tau}\equiv Q$.*

As corollaries of Theorem 9 and Lemma 10, we get that the transition system is image-finite, and that the reduction relation is image-finite up to structural congruence:

Lemma 10 *For all P and α, the set $\{R : P \xrightarrow{\alpha} R\}$ is finite.*

Proof By induction on the structure of P. □

Lemma 11 *For all P, the set $\{\{R : Q \equiv R\} : P \to Q\}$ is finite.*

Proof By Lemma 10, the set $\{Q : P \xrightarrow{\tau} Q\}$ is finite. Therefore, the set $\{\{R : Q \equiv R\} : P \xrightarrow{\tau} Q\}$ is finite. But, by Theorem 9 and the transitivity of structural congruence this set is the same as $\{\{R : Q \equiv R\} : P \to Q\}$. □

4.3 A Context Lemma

The context lemma presented in this section is a tool for proving contextual equivalence by considering only a limited set of contexts, rather than all contexts. Many context lemmas have been proved for a wide range of calculi, starting with Milner's context lemma for the combinatory logic form of PCF [10].

Our context lemma is stated in terms of a notion of a *harness*:

Harnesses:

$H ::=$	harnesses
$-$	process variable
$(\nu n)H$	restriction
$P \mid H$	left composition
$H \mid Q$	right composition
$n[H]$	ambient

Harnesses are analogous to the evaluation contexts found in context lemmas for some other calculi. Unlike the contexts of Section 3, harnesses are identified up to consistent renaming of bound names. We let $\mathit{fn}(H)$ and $\mathit{fv}(H)$ be the sets of names and variables, respectively, occurring free in a harness H. There is exactly one occurrence of the process variable $-$ in any harness. If H is an harness, we write $H\{P\}$ for the outcome of substituting the process P for the single occurrence of the process variable $-$. Names restricted in H are renamed to avoid capture of free names of P. For example, if $H = (\nu n)(- \mid \mathit{open}\, n)$ then $H\{n[]\} = (\nu n')(n[] \mid \mathit{open}\, n')$ for some $n' \neq n$.

Let a *substitution*, σ, be a list $x_1{\leftarrow}M_1, \ldots, x_k{\leftarrow}M_k$, where the variables x_1, $\ldots$, x_k are pairwise distinct, and $\mathit{fv}(M_i) = \varnothing$ for each $i \in 1..k$. Let $\mathit{dom}(\sigma) = \{x_1, \ldots, x_k\}$. Let $P\sigma$ be the process $P\{x_1{\leftarrow}M_1\} \cdots \{x_k{\leftarrow}M_k\}$. Let a process or a harness be *closed* if and only if it has no free variables (though it may have free names).

Here is our context lemma:

Theorem 12 (Context) *For all processes P and Q, $P \simeq Q$ if and only if for all substitutions σ with $\mathit{dom}(\sigma) = \mathit{fv}(P) \cup \mathit{fv}(Q)$, and for all closed harnesses H and names n, that $H\{P\sigma\} \Downarrow n \Leftrightarrow H\{Q\sigma\} \Downarrow n$.*

A corollary is that for all closed processes P and Q, $P \simeq Q$ if and only if for all closed harnesses H and names n, that $H\{P\} \Downarrow n \Leftrightarrow H\{Q\} \Downarrow n$.

In general, however, we need to consider the arbitrary closing substitution σ when using Theorem 12. This is because a variable free in a process may become bound to an expression once the process is placed in a context. For example, let $P = x[n[]] \mid \mathit{open}\, y.\mathbf{0}$ and $Q = \mathbf{0}$. Consider the context $\mathcal{C}() = \langle m, m\rangle \mid (x, y).()$. We have $\mathcal{C}(P) \Downarrow n$ but not $\mathcal{C}(Q) \Downarrow n$. So P and Q are not contextually equivalent but they do satisfy $H\{P\} \Downarrow n \Leftrightarrow H\{Q\} \Downarrow n$ for all closed H and n.

Some process calculi enjoy stronger context lemmas. Let processes P and Q be *parallel testing equivalent* if and only if for all processes R and names n, that $P \mid R \Downarrow n \Leftrightarrow Q \mid R \Downarrow n$. We might like to show that any two closed processes are contextually equivalent if and only if they are parallel testing equivalent. This would be a stronger result than Theorem 12 because it would avoid considering contexts that include ambients. Such a result is true for CCS [9], for example, but it is false for the ambient calculus. To see this, let $P = \mathit{out}\, p.\mathbf{0}$ and $Q = \mathbf{0}$. We may show that $P \mid R \Downarrow n \Leftrightarrow Q \mid R \Downarrow n$ for all n and R. Now, consider the context $\mathcal{C}() = p[m[()]]$. We have $\mathcal{C}(P) \Downarrow m$ but not $\mathcal{C}(\mathbf{0}) \Downarrow m$. So P and Q are parallel testing equivalent but not contextually equivalent.

4.4 An Activity Lemma

When we come to apply Theorem 12 we need to analyze judgments of the form $H\{P\} \downarrow n$ or $H\{P\} \rightarrow Q$. In this section we formalize these analyses.

We begin by extending the structural congruence, hardening, and reduction relations to harnesses as follows:

- Let $H \equiv H'$ hold if and only if $H\{P\} \equiv H'\{P\}$ for all P.

- Let $H > (\nu\vec{p})\langle n[H']\rangle Q$ hold if and only if $H\{P\} > (\nu\vec{p})\langle n[H'\{P\}]\rangle Q$ for all P such that $\{\vec{p}\} \cap fn(P) = \varnothing$.
- Let $H > (\nu\vec{p})\langle Q\rangle H'$ hold if and only if $H\{P\} > (\nu\vec{p})\langle Q\rangle(H'\{P\})$ for all P such that $\{\vec{p}\} \cap fn(P) = \varnothing$.
- Let $H \rightarrow H'$ hold if and only if, for all P, $H\{P\} \rightarrow H'\{P\}$.

We need the following lemma about hardening:

Lemma 13 *If $H\{P\} > (\nu\vec{p})\langle P_1\rangle P_2$ then either:*

(1) *$H > (\nu\vec{p})\langle n[H']\rangle P_2$ and $P_1 = n[H'\{P\}]$, or*

(2) *$H > (\nu\vec{p})\langle P_1\rangle H'$ and $P_2 = H'\{P\}$, or*

(3) *$P > (\nu\vec{p})\langle P_1\rangle P'$, $H \equiv - \mid R$, $P_2 \equiv P' \mid R$, and $\{\vec{p}\} \cap fn(R) = \varnothing$.*

Intuitively, there are two ways in which $H\{P\} \downarrow n$ can arise: either the process P exhibits the name by itself, or the harness H exhibits the name n by itself. Proposition 14 formalizes this analysis. Similarly, there are three ways in which a reduction $H\{P\} \rightarrow Q$ may arise: either (1) the process P reduces by itself, or (2) the harness H reduces by itself, or (3) there is an interaction between the process and the harness. Theorem 15 formalizes this analysis. Such a result is sometimes known as an activity lemma [16].

Proposition 14 *If $H\{P\} \downarrow n$ then either (1) $H\{Q\} \downarrow n$ for all Q, or (2) both $P \downarrow n$ and also for all Q, $Q \downarrow n$ implies that $H\{Q\} \downarrow n$.*

Proof By Proposition 7, $H\{P\} \downarrow n$ means there are $\vec{p}$, P', P'' such that $H\{P\} > (\nu\vec{p})\langle n[P']\rangle P''$ with $n \notin \{\vec{p}\}$. Hence, the proposition follows from Lemma 13. □

Theorem 15 (Activity) *$H\{P\} \rightarrow R$ if and only if:*

(Act Proc) *there is a reduction $P \rightarrow P'$ with $R \equiv H\{P'\}$, or*

(Act Har) *there is a reduction $H \rightarrow H'$ with $R \equiv H'\{P\}$, or*

(Act Inter) *there are H' and $\vec{r}$ with $\{\vec{r}\} \cap fn(P) = \varnothing$, and one of the following holds:*

(Inter In) *$H \equiv (\nu\vec{r})H'\{m[- \mid R'] \mid n[R'']\}$, $P \xrightarrow{in\ n} P'$, and $R \equiv (\nu\vec{r})H'\{n[m[P' \mid R'] \mid R'']\}$*

(Inter Out) *$H \equiv (\nu\vec{r})H'\{n[m[- \mid R'] \mid R'']\}$, $P \xrightarrow{out\ n} P'$, and $R \equiv (\nu\vec{r})H'\{m[P' \mid R'] \mid n[R'']\}$*

(Inter Open) *$H \equiv (\nu\vec{r})H'\{- \mid n[R']\}$, $P \xrightarrow{open\ n} P'$, and $R \equiv (\nu\vec{r})H'\{P' \mid R'\}$*

(Inter Input) *$H \equiv (\nu\vec{r})H'\{- \mid \langle M\rangle\}$, $P > (\nu\vec{p})\langle(x).P'\rangle P''$, and $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(P'\{x\leftarrow M\} \mid P'')\}$, with $\{\vec{p}\} \cap fn(M) = \varnothing$*

(Inter Output) $H \equiv (\nu\vec{r})H'\{- \mid (x).R'\}$, $P > (\nu\vec{p})\langle\langle M\rangle\rangle P'$, *and* $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(P' \mid R'\{x{\leftarrow}M\})\}$, *with* $\{\vec{p}\} \cap \mathit{fn}(R') = \varnothing$

(Inter Amb) $P > (\nu\vec{p})\langle n[Q]\rangle P'$ *and one of the following holds:*

(1) $Q \xrightarrow{in\ m} Q'$, $H \equiv (\nu\vec{r})H'\{- \mid m[R']\}$, $\{\vec{p}\} \cap \mathit{fn}(m[R']) = \varnothing$,
and $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(P' \mid m[n[Q'] \mid R'])\}$

(2) $Q \xrightarrow{out\ m} Q'$, $H \equiv (\nu\vec{r})H'\{m[- \mid R']\}$, $m \notin \{\vec{p}\}$,
and $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(n[Q'] \mid m[P' \mid R'])\}$

(3) $H \equiv (\nu\vec{r})H'\{m[R' \mid \mathit{in}\, n.R''] \mid -\}$, $\{\vec{p}\} \cap \mathit{fn}(m[R' \mid \mathit{in}\, n.R'']) = \varnothing$,
and $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(n[Q \mid m[R' \mid R'']] \mid P')\}$

(4) $H \equiv (\nu\vec{r})H'\{- \mid \mathit{open}\, n.R'\}$, $n \notin \{\vec{p}\}$,
and $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(Q \mid P') \mid R'\}$

5 Examples of Contextual Equivalence

In this section, three examples demonstrate how we can apply Theorem 12 and Theorem 15 to establish contextual equivalence.

5.1 Opening an Ambient

First, we return to and prove Example 3 from Section 3.

Lemma 16 *If* $H\{(\nu n)(n[] \mid \mathit{open}\, n.P)\} \Downarrow m$ *and* $n \notin \mathit{fn}(P)$ *then* $H\{P\} \Downarrow m$.

Proof By induction on the derivation of $H\{(\nu n)(n[] \mid \mathit{open}\, n.P)\} \Downarrow m$:

(Conv Exh) Here $H\{(\nu n)(n[] \mid \mathit{openn}.P)\} \downarrow m$. By Proposition 14, either (1), for all Q, $H\{Q\} \downarrow m$, or (2), $(\nu n)(n[] \mid \mathit{open}\, n.P) \downarrow m$. In case (1), we have, in particular, that $H\{P\} \downarrow m$. Hence, $H\{P\} \Downarrow m$, by (Conv Exh). Case (2) cannot arise, since, by Proposition 7, $(\nu n)(n[] \mid \mathit{open}\, n.P) \downarrow m$ implies that $(\nu n)(n[] \mid \mathit{open}\, n.P) > (\nu\vec{p})\langle m[P']\rangle P''$ with $m \notin \{\vec{p}\}$. But the only hardenings of the process $(\nu n)(n[] \mid \mathit{open}\, n.P)$ are:

$$\begin{array}{rcl}
(\nu n)(n[] \mid \mathit{open}\, n.P) & > & (\nu n)\langle n[]\rangle(\mathbf{0} \mid \mathit{open}\, n.P) \\
(\nu n)(n[] \mid \mathit{open}\, n.P) & > & (\nu n)\langle \mathit{open}\, n.P\rangle(n[] \mid \mathbf{0})
\end{array}$$

So case (2) is impossible.

(Conv Red) Here $H\{(\nu n)(n[] \mid \mathit{open}\, n.P)\} \to R$ and $R \Downarrow m$. By Theorem 15, one of three cases pertains:

(Act Proc) Then $(\nu n)(n[] \mid \mathit{open}\, n.P) \to P'$ with $R \equiv H\{P'\}$. By inspection of the rules of the labelled transition system, it must be that (Trans Open) derives this transition, with $P' \equiv P$. Therefore $R \Downarrow m$ implies that $H\{P\} \Downarrow m$.

(Act Har) Then $H \rightarrow H'$ with $R \equiv H'\{(\nu n)(n[] \mid \mathit{open}\, n.P)\}$. By Lemma 2, we may derive $H'\{(\nu n)(n[] \mid \mathit{open}\, n.P)\} \Downarrow m$ by the same depth of inference as $R \Downarrow m$. By induction hypothesis, $H'\{P\} \Downarrow m$. From $H \rightarrow H'$ we obtain $H\{P\} \rightarrow H'\{P\}$ in particular. By (Act Har), we get $H\{P\} \Downarrow m$.

(Act Inter) Then there is an interaction between the process $(\nu n)(n[] \mid \mathit{open}\, n.P)$ and the harness H. Given the possible hardenings of $(\nu n)(n[] \mid \mathit{open}\, n.P)$ stated above, none of the possibilities stated in clause (Act Inter) of Theorem 15 pertains. So this case is impossible. □

Proof of Example 3 *$(\nu n)(n[] \mid \mathit{open}\, n.P) \simeq P$ if $n \notin \mathit{fn}(P)$.*

Proof By Theorem 12, it suffices to prove $H\{((\nu n)(n[] \mid \mathit{openn}.P))\sigma\} \Downarrow m \Leftrightarrow H\{P\sigma\} \Downarrow m$ for all closed harnesses H and names m and for all substitutions σ with $\mathit{dom}(\sigma) = \mathit{fv}(P)$. Since the name n is bound, we may assume that $n \notin \mathit{fn}(\sigma(x))$ for all $x \in \mathit{dom}(\sigma)$. Therefore, we are to prove that: $H\{(\nu n)(n[] \mid \mathit{open}\, n.P\sigma\} \Downarrow m \Leftrightarrow H\{P\sigma\} \Downarrow m$ where $n \notin \mathit{fn}(P\sigma)$.

We prove each direction separately. First, suppose that $H\{P\sigma\} \Downarrow m$. Since $(\nu n)(n[] \mid \mathit{open}\, n.P\sigma) \rightarrow P\sigma$, we get $H\{(\nu n)(n[] \mid \mathit{open}\, n.P\sigma)\} \rightarrow H\{P\sigma\}$. By (Conv Red), we get $H\{(\nu n)(n[] \mid \mathit{open}\, n.P\sigma)\} \Downarrow m$. Second, suppose that $H\{(\nu n)(n[] \mid \mathit{open}\, n.P\sigma)\} \Downarrow m$. By Lemma 16, we get $H\{P\sigma\} \Downarrow m$. □

5.2 The Perfect Firewall Equation

Consider a process $(\nu n)n[P]$, where n is not free in P. Since the name n is known neither inside the ambient $n[P]$, nor outside it, the ambient $n[P]$ is a "perfect firewall" that neither allows another ambient to enter nor to exit. The following two lemmas allow us to prove that $(\nu n)n[P]$ is contextually equivalent to $\mathbf{0}$, when $n \notin \mathit{fn}(P)$, which is to say that no context can detect the presence of $(\nu n)n[P]$.

Lemma 17 *If $H\{(\nu n)n[P]\} \Downarrow m$ and $n \notin \mathit{fn}(P)$ then $H\{\mathbf{0}\} \Downarrow m$.*

Proof By induction on the derivation of $H\{(\nu n)n[P]\} \Downarrow m$.

(Conv Exh) Here $H\{(\nu n)n[P]\} \downarrow m$. By Proposition 14, either (1), for all Q, $H\{Q\} \downarrow m$, or (2), $(\nu n)n[P] \downarrow m$. In case (1), we have, in particular, that $H\{\mathbf{0}\} \downarrow m$. Hence, $H\{\mathbf{0}\} \Downarrow m$, by (Conv Exh). Case (2) cannot arise, since, by Proposition 7, $(\nu n)n[P] \downarrow m$ implies that $(\nu n)n[P] > (\nu \vec{p})\langle m[P']\rangle P''$ with $m \notin \{\vec{p}\}$, which is impossible.

(Conv Red) Here $H\{(\nu n)n[P]\} \rightarrow R$ and $R \Downarrow m$. By Theorem 15, one of three cases pertains:

(Act Proc) Then $(\nu n)n[P] \rightarrow P''$ with $R \equiv H\{P''\}$. By Theorem 9, there is Q with $(\nu n)n[P] \xrightarrow{\tau} Q$ and $Q \equiv P''$. Since $(\nu n)n[P] >$

$(\nu n)\langle n[P]\rangle\mathbf{0}$ is the only hardening derivable from $(\nu n)n[P]$, the transition $(\nu n)n[P] \xrightarrow{\tau} Q$ can only be derived using (Trans Amb), with $P \xrightarrow{\tau} P'$ and $Q = (\nu n)(n[P'] \mid \mathbf{0})$. Therefore, there is a reduction $P \rightarrow P'$ and $P'' \equiv (\nu n)n[P']$. By Lemma 21 stated in the Appendix, $P \rightarrow P'$ implies $fn(P') \subseteq fn(P)$ and so $n \notin fn(P')$. We have $R \equiv H\{(\nu n)n[P']\}$ with $n \notin fn(P')$. By Lemma 2, we may derive $H\{(\nu n)n[P']\} \Downarrow m$ by the same depth of inference as $R \Downarrow m$. By induction hypothesis, $H\{\mathbf{0}\} \Downarrow m$.

(Act Har) Then $H \rightarrow H'$ with $R \equiv H'\{(\nu n)n[P]\}$. By Lemma 2, we may derive $H'\{(\nu n)n[P]\} \Downarrow m$ by the same depth of inference as $R \Downarrow m$. By induction hypothesis, $H'\{\mathbf{0}\} \Downarrow m$. From $H \rightarrow H'$ we obtain $H\{\mathbf{0}\} \rightarrow H'\{\mathbf{0}\}$ in particular. By (Conv Red), we get $H\{\mathbf{0}\} \Downarrow m$.

(Act Inter) Then there are H' and $\vec{r}$ with $\{\vec{r}\} \cap fn(P) = \varnothing$ and one of several conditions must hold. Since the only hardening or transition from $(\nu n)n[P]$ is $(\nu n)n[P] > (\nu n)\langle n[P]\rangle\mathbf{0}$, only the rule (Inter Amb) applies. According to Theorem 15, there are four possibilities to consider.

(1) Here, $P \xrightarrow{in\ m} P'$, $H \equiv (\nu\vec{r})H'\{- \mid m[R']\}$, $\{n\} \cap fn(m[R']) = \varnothing$, and $R \equiv (\nu\vec{r})H'\{(\nu n)(\mathbf{0} \mid m[n[P'] \mid R'])\}$. We have $R \equiv (\nu\vec{r})H'\{m[R' \mid (\nu n)n[P']]\}$. By Lemma 23 (stated in the Appendix), $n \notin fn(P)$ and $P \xrightarrow{in\ m} P'$ imply $n \notin fn(P')$. By Lemma 2, we get $(\nu\vec{r})H'\{m[R' \mid (\nu n)n[P']]\} \Downarrow m$ with the same depth of inference as $R \Downarrow m$. By induction hypothesis, $(\nu\vec{r})H'\{m[R' \mid \mathbf{0}]\} \Downarrow m$. Moreover, $H\{\mathbf{0}\} \equiv (\nu\vec{r})H'\{m[R' \mid \mathbf{0}]\}$, and therefore $H\{\mathbf{0}\} \Downarrow m$.

(2) Here, $P \xrightarrow{out\ m} P'$, $H \equiv (\nu\vec{r})H'\{m[- \mid R']\}$, $m \notin \{n\}$, and also $R \equiv (\nu\vec{r})H'\{(\nu n)(n[P'] \mid m[\mathbf{0} \mid R'])\}$. We have $R \equiv (\nu\vec{r})H'\{m[R'] \mid (\nu n)n[P']\}$. By Lemma 23, $n \notin fn(P)$ and $P \xrightarrow{out\ m} P'$ imply $n \notin fn(P')$. Lemma 2 implies $(\nu\vec{r})H'\{m[R'] \mid (\nu n)n[P']\} \Downarrow m$ with the same depth of inference as $R \Downarrow m$. By induction hypothesis, $(\nu\vec{r})H'\{m[R'] \mid \mathbf{0}\} \Downarrow m$. Moreover, $H\{\mathbf{0}\} \equiv (\nu\vec{r})H'\{m[R'] \mid \mathbf{0}\}$ and therefore $H\{\mathbf{0}\} \Downarrow m$.

The other possibilities, (3) and (4), are ruled out because the name n is restricted in the concretion $(\nu n)\langle n[P]\rangle\mathbf{0}$. □

Lemma 18 *If* $H\{\mathbf{0}\} \Downarrow m$ *then* $H\{P\} \Downarrow m$.

Proof By induction on the derivation of $H\{\mathbf{0}\} \Downarrow m$.

(Conv Exh) Here $H\{\mathbf{0}\} \downarrow m$. By Proposition 14, either (1), for all Q, $H\{Q\} \downarrow m$, or (2), $\mathbf{0} \downarrow m$. Case (2) is impossible. In case (1), we get, in particular, that $H\{P\} \downarrow m$. Hence, $H\{P\} \Downarrow m$.

(Conv Red) Here $H\{\mathbf{0}\} \to Q$ and $Q \Downarrow m$. By Theorem 15, and the fact that $\mathbf{0}$ has no reductions and no hardenings, it must be that $H \to H'$ with $Q \equiv H'\{\mathbf{0}\}$. By Lemma 2, we get that $H'\{\mathbf{0}\} \Downarrow m$ is derivable with the same depth of inference as $Q \Downarrow m$. By induction hypothesis, $H'\{P\} \Downarrow m$. From $H \to H'$ we get that $H\{P\} \to H'\{P\}$. By (Conv Red), $H\{P\} \to H'\{P\}$ and $H'\{P\} \Downarrow m$ imply $H\{P\} \Downarrow m$. □

Using these two lemmas we get:

Example 4 *If $n \notin fn(P)$ then $(\nu n)n[P] \simeq \mathbf{0}$.*

Proof By Theorem 12, it suffices to prove that

$$H\{((\nu n)n[P])\sigma\} \Downarrow m \Leftrightarrow H\{\mathbf{0}\sigma\} \Downarrow m$$

for all closed harnesses H and names m and for all substitutions σ such that $dom(\sigma) = fv((\nu n)n[P])$. Since the name n is bound, we may assume that $n \notin fn(\sigma(x))$ for any $x \in dom(\sigma)$. Therefore, we are to prove that:

$$H\{(\nu n)n[P\sigma]\} \Downarrow m \Leftrightarrow H\{\mathbf{0}\} \Downarrow m$$

where $n \notin fn(P\sigma)$. This follows from Lemma 17 and Lemma 18. □

Our first proof of this equation (which was stated in an earlier paper [7]) was by a direct quantification over all contexts. The proof above using the context lemma is simpler.

5.3 Crossing a Firewall

This example concerns an agent that crosses a firewall using previously arranged passwords. We explained this example, but did not state a proof, in an earlier paper [7].

Lemma 19 *Suppose that $(fn(P) \cup fn(Q)) \cap \{k, k', k''\} = \varnothing$ and $w \notin fn(Q)$. Consider the processes defined by:*

$$\begin{aligned}
R_1 &\triangleq (\nu k\, k'\, k'')(k'[open\ k.k''[Q]] \mid \\
&\qquad\qquad (\nu w)w[k[out\ w.in\ k'.in\ w] \mid open\ k'.open\ k''.P]) \\
R_2 &\triangleq (\nu k\, k'\, k''\, w)(k'[open\ k.k''[Q]] \mid k[in\ k'.in\ w] \mid w[open\ k'.open\ k''.P]) \\
R_3 &\triangleq (\nu k\, k'\, k''\, w)(k'[k[in\ w] \mid open\ k.k''[Q]] \mid w[open\ k'.open\ k''.P]) \\
R_4 &\triangleq (\nu k\, k'\, k''\, w)(k'[in\ w \mid k''[Q]] \mid w[open\ k'.open\ k''.P]) \\
R_5 &\triangleq (\nu k\, k'\, k''\, w)w[k'[k''[Q]] \mid open\ k'.open\ k''.P] \\
R_6 &\triangleq (\nu k\, k'\, k''\, w)w[k''[Q] \mid open\ k''.P] \\
R_7 &\triangleq (\nu w)w[Q \mid P]
\end{aligned}$$

For each $i \in 1..6$, $R_i \simeq R_{i+1}$.

Proof Suppose that $i \in 1..6$. Without loss of generality, we may assume that the processes P and Q are closed, and hence that all the R_i are closed. By Theorem 12, we need to show for all H and m that $H\{R_i\} \Downarrow m \Leftrightarrow H\{R_{i+1}\} \Downarrow m$. We may calculate that $R_i \rightarrow R_{i+1}$, for each i. It follows that $H\{R_{i+1}\} \Downarrow m$ implies $H\{R_i\} \Downarrow m$.

We now prove that $H\{R_i\} \Downarrow m$ implies $H\{R_{i+1}\} \Downarrow m$ by induction on the derivation of $H\{R_i\} \Downarrow m$.

(Conv Exh) Here $H\{R_i\} \downarrow m$. By Proposition 14, either (1), for all Q, $H\{Q\} \downarrow m$, or (2), $R_i \downarrow m$. In case (1), we have, in particular, that $H\{R_{i+1}\} \downarrow m$. Hence, $H\{R_{i+1}\} \Downarrow m$, by (Conv Exh). Case (2) cannot arise, because of the outermost restrictions on each R_i.

(Conv Red) Here $H\{R_i\} \rightarrow R$ and $R \downarrow m$. By Theorem 9 and Theorem 15, one of three cases pertains:

(Act Proc) Then $R_i \rightarrow R'$ with $R \equiv H\{R'\}$. By inspection of the definitions of R_i and the labelled transition system, it must be that $R' \equiv R_{i+1}$. Therefore $R \Downarrow m$ implies that $H\{R_{i+1}\} \Downarrow m$.

(Act Har) Then $H \rightarrow H'$ with $R \equiv H'\{R_i\}$. By Lemma 2, we may derive $H'\{R_i\} \Downarrow m$ by the same depth of inference as $R \Downarrow m$. By induction hypothesis, $H'\{R_{i+1}\} \Downarrow m$. From $H \rightarrow H'$ we obtain $H\{R_{i+1}\} \rightarrow H'\{R_{i+1}\}$ in particular. By (Conv Red), we get $H\{R_{i+1}\} \Downarrow m$.

(Act Inter) Then there is an interaction between the process R_i and the harness H'. Given that $fn(Q) \cap \{k', k'', w\} = \varnothing$, none of the conditions stated in the rule (Act Inter) of Theorem 15 applies. Therefore this case is impossible.

This completes the proof by induction. □

Example 5 *Let us define:*

$$\begin{array}{rcl} \mathit{Firewall} & \triangleq & (\nu w)w[k[\mathit{out}\ w.\mathit{in}\ k'.\mathit{in}\ w] \mid \mathit{open}\ k'.\mathit{open}\ k''.P] \\ \mathit{Agent} & \triangleq & k'[\mathit{open}\ k.k''[Q]] \end{array}$$

If $(fn(P) \cup fn(Q)) \cap \{k, k', k''\} = \varnothing$ *and* $w \notin fn(Q)$ *then:*

$$(\nu k\, k'\, k'')(\mathit{Agent} \mid \mathit{Firewall}) \quad \simeq \quad (\nu w)w[Q \mid P]$$

Proof Recall the processes R_1 and R_7 from Lemma 19. By that lemma, $R_1 \simeq R_7$. This is exactly the desired equation, since $R_1 = (\nu k\ k'\ k'')(\mathit{Agent} \mid \mathit{Firewall})$ and $R_7 = (\nu w)w[Q \mid P]$. □

6 Conclusions

We developed a theory of Morris-style contextual equivalence for the ambient calculus. We showed that standard tools such as a labelled transition system, a context lemma, and an activity lemma, may be adapted to the ambient calculus. We introduced a new technique, based on a hardening relation, for defining the labelled transition system. We employed these tools to prove equational properties of mobile ambients.

Our use of concretions to highlight those subprocesses of a process that may participate in a computation follows Milner [11, 12], and is an alternative to the use of membranes and airlocks in the chemical abstract machine of Berry and Boudol [5]. Unlike these authors, in the definition of our transition relation we use the hardening relation, rather than the full structural congruence relation, to choose subprocesses to participate in a transition. In applications of the activity lemma, Theorem 15, and in other situations, our proof techniques depend on analyzing the possible hardenings and the possible transitions of processes by examining their structure. This is possible because, unlike structural congruence, the hardening relation is not transitive. Therefore, the use of hardening rather than structural congruence in the definition of the transition relation is essential for the techniques we advocate here.

Our use of the hardening relation to define the transition relation for the ambient calculus is similar to the use by Vitek and Castagna [19] of a heating relation to define reduction in their Seal calculus. A difference in style is that Vitek and Castagna use structural congruence as well as the heating relation to define their reduction relation.

In the future, it would be of interest to study bisimulation of ambients. Various techniques adopted for higher-order [14, 18] and distributed [3, 4, 17] variants of the π-calculus may be applicable to the ambient calculus.

Acknowledgement Comments by Cédric Fournet, Georges Gonthier, and Tony Hoare were helpful.

References

[1] M. Abadi, C. Fournet, and G. Gonthier. Secure implementation of channel abstractions. In *Proceedings LICS'98*, pages 105–116, 1998.

[2] M. Abadi and A. D. Gordon. A calculus for cryptographic protocols: The spi calculus. *Information and Computation*, 148:1–70, 1999.

[3] R. M. Amadio. An asynchronous model of locality, failure, and process mobility. In *Proceedings COORDINATION 97*, volume 1282 of *Lecture Notes in Computer Science*. Springer-Verlag, 1997.

[4] R. M. Amadio and S. Prasad. Localities and failures. In *Proceedings FST&TCS'94*, volume 880 of *Lecture Notes in Computer Science*, pages 205–216. Springer-Verlag, 1994.

[5] G. Berry and G. Boudol. The chemical abstract machine. *Theoretical Computer Science*, 96(1):217–248, April 1992.

[6] L. Cardelli. Abstractions for mobile computation. In C. Jensen and J. Vitek, editors, *Secure Internet Programming: Issues in Distributed and Mobile Object Systems*, volume 1603 of *Lecture Notes in Computer Science*. Springer-Verlag, 1999.

[7] L. Cardelli and A. D. Gordon. Mobile ambients. In *Foundations of Software Science and Computation Structures*, volume 1378 of *Lecture Notes in Computer Science*, pages 140–155. Springer-Verlag, 1998.

[8] L. Cardelli and A. D. Gordon. Types for mobile ambients. In *Proceedings POPL'99*, pages 79–92, January 1999.

[9] R. De Nicola and M. C. B. Hennessy. Testing equivalences for processes. *Theoretical Computer Science*, 34:83–133, 1984.

[10] R. Milner. Fully abstract models of typed lambda-calculi. *Theoretical Computer Science*, 4:1–23, 1977.

[11] R. Milner. The polyadic π-calculus: A tutorial. Technical Report ECS–LFCS–91–180, Laboratory for Foundations of Computer Science, Department of Computer Science, University of Edinburgh, October 1991.

[12] R. Milner. The π-calculus. Undergraduate lecture notes, Cambridge University, 1995.

[13] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, parts I and II. *Information and Computation*, 100:1–40 and 41–77, 1992.

[14] R. Milner and D. Sangiorgi. Barbed bisimulation. In *Proceedings ICALP '92*, volume 623 of *Lecture Notes in Computer Science*. Springer-Verlag, 1992.

[15] J. H. Morris. *Lambda-Calculus Models of Programming Languages*. PhD thesis, MIT, December 1968.

[16] G. D. Plotkin. LCF considered as a programming language. *Theoretical Computer Science*, 5:223–255, 1977.

[17] J. Riely and M. Hennessy. A typed language for distributed mobile processes. In *Proceedings POPL'98*, pages 378–390, 1998.

[18] D. Sangiorgi. *Expressing Mobility in Process Algebras: First-Order and Higher-Order Paradigms*. PhD thesis, University of Edinburgh, 1992.

[19] J. Vitek and G. Castagna. Seal: A framework for secure mobile computations. In *Internet Programming Languages*, Lecture Notes in Computer Science. Springer-Verlag, 1999. To appear.

A Proofs

In this appendix, we prove all the propositions stated without proof in the main body of the paper. To do so, we need several auxiliary results.

The appendix consists of several sections.

(1) In Section A.1 we prove that contextual equivalence is a congruence, which was stated in Section 3.

(2) In Section A.2, we prove three important facts about the hardening relation, Lemma 5, Proposition 6, and Proposition 7, which were stated in Section 4.1.

(3) Section A.3 contains some auxiliary results and a proof of Theorem 9 from Section 4.2, the result which states that the reduction and τ-transition relations are the same up to structural congruence.

(4) In Section A.4 we prove the activity lemma, Theorem 15, stated in Section 4.4.

(5) In Section A.5, we prove some auxiliary results about replication.

(6) Section A.6 is devoted to proving our context lemma, Theorem 12, which was stated in Section 4.3.

In the main text, we stated Theorem 12 ahead of Theorem 15, but in fact we use Theorem 15 in the proof of Theorem 12. Therefore, we give the proof of Theorem 15 before the proof of Theorem 12.

Throughout this appendix, we shall refer to the rules of structural congruence and reduction using the names in the following tables:

Structural Congruence: $P \equiv Q$

$P \equiv P$	(Struct Refl)
$Q \equiv P \Rightarrow P \equiv Q$	(Struct Symm)
$P \equiv Q, Q \equiv R \Rightarrow P \equiv R$	(Struct Trans)
$P \equiv Q \Rightarrow (\nu n)P \equiv (\nu n)Q$	(Struct Res)
$P \equiv Q \Rightarrow P \mid R \equiv Q \mid R$	(Struct Par)
$P \equiv Q \Rightarrow !P \equiv !Q$	(Struct Repl)
$P \equiv Q \Rightarrow M[P] \equiv M[Q]$	(Struct Amb)
$P \equiv Q \Rightarrow M.P \equiv M.Q$	(Struct Action)
$P \equiv Q \Rightarrow (x).P \equiv (x).Q$	(Struct Input)
$P \mid Q \equiv Q \mid P$	(Struct Par Comm)
$(P \mid Q) \mid R \equiv P \mid (Q \mid R)$	(Struct Par Assoc)
$!P \equiv P \mid !P$	(Struct Repl Par)
$(\nu n)(\nu m)P \equiv (\nu m)(\nu n)P$	(Struct Res Res)
$n \notin fn(P) \Rightarrow (\nu n)(P \mid Q) \equiv P \mid (\nu n)Q$	(Struct Res Par)
$n \neq m \Rightarrow (\nu n)m[P] \equiv m[(\nu n)P]$	(Struct Res Amb)

$P \mid \mathbf{0} \equiv P$	(Struct Zero Par)
$(\nu n)\mathbf{0} \equiv \mathbf{0}$	(Struct Zero Res)
$!\mathbf{0} \equiv \mathbf{0}$	(Struct Zero Repl)
$\epsilon.P \equiv P$	(Struct ϵ)
$(M.M').P \equiv M.M'.P$	(Struct .)

Reduction: $P \rightarrow Q$

$n[\mathit{in}\, m.P \mid Q] \mid m[R] \rightarrow m[n[P \mid Q] \mid R]$	(Red In)
$m[n[\mathit{out}\, m.P \mid Q] \mid R] \rightarrow n[P \mid Q] \mid m[R]$	(Red Out)
$\mathit{open}\, n.P \mid n[Q] \rightarrow P \mid Q$	(Red Open)
$\langle M \rangle \mid (x).P \rightarrow P\{x \leftarrow M\}$	(Red I/O)
$P \rightarrow Q \Rightarrow P \mid R \rightarrow Q \mid R$	(Red Par)
$P \rightarrow Q \Rightarrow (\nu n)P \rightarrow (\nu n)Q$	(Red Res)
$P \rightarrow Q \Rightarrow n[P] \rightarrow n[Q]$	(Red Amb)
$P' \equiv P, P \rightarrow Q, Q \equiv Q' \Rightarrow P' \rightarrow Q'$	(Red $\equiv$)

Many of the proofs in the rest of the appendix depend on the following basic facts about structural congruence, reduction, hardening, and the transition relation:

Lemma 20 *If $P \equiv Q$ then $\mathit{fn}(P) = \mathit{fn}(Q)$ and $\mathit{fv}(P) = \mathit{fv}(Q)$.*

Lemma 21 *If $P \rightarrow Q$ then $\mathit{fn}(Q) \subseteq \mathit{fn}(P)$ and $\mathit{fv}(Q) \subseteq \mathit{fv}(P)$.*

Lemma 22 *If $P > C$ then $\mathit{fn}(P) = \mathit{fn}(C)$ and $\mathit{fv}(P) = \mathit{fv}(Q)$.*

Lemma 23 *If $P \xrightarrow{\alpha} P'$ then $\mathit{fn}(\alpha) \cup \mathit{fn}(P') \subseteq \mathit{fn}(P)$, $\mathit{fv}(\alpha) = \varnothing$, and $\mathit{fv}(P') \subseteq \mathit{fv}(P)$.*

Lemma 24 *If $n \notin \mathit{fn}(P)$ then $(\nu n)P \equiv P$.*

Proof Using the axioms (Struct Zero Par), (Struct Res Par), and (Struct Zero Res), we get: $(\nu n)P \equiv (\nu n)(P \mid \mathbf{0}) \equiv P \mid (\nu n)\mathbf{0} \equiv P \mid \mathbf{0} \equiv P$. □

A.1 Proof Omitted From Section 3

Apart from proving transitivity, the proof that contextual equivalence is a congruence is easy:

Proof of Proposition 1 *Contextual equivalence is a congruence.*

Proof Reflexivity and symmetry are trivial.

For transitivity, suppose that $P \simeq P'$ and $P' \simeq P''$. To show that $P \simeq P''$, consider any context $\mathcal{C}()$ and any name n such that $\mathcal{C}(P)$ and $\mathcal{C}(P'')$ are closed. It need not be that $\mathcal{C}(P')$ is closed. Suppose that $\{x_1, \ldots, x_k\} = \mathit{fv}(\mathcal{C}(P'))$, and suppose that $m_1, \ldots, m_k$ are fresh names. We define a new family of contexts

$\mathcal{D}_0$, $\mathcal{D}_1$, $\ldots$, $\mathcal{D}_k$ by induction: $\mathcal{D}_0 = \mathcal{C}$ and $\mathcal{D}_{i+1} = \langle m_{i+1} \rangle \mid (x_{i+1}).\mathcal{D}_i$. The context $\mathcal{D}_k$ has two useful properties. First, for all Q and q,

$$\mathcal{D}_k(Q) \Downarrow q \Leftrightarrow \mathcal{C}(Q)\{x_1 \leftarrow m_1\} \cdots \{x_k \leftarrow m_k\} \Downarrow q$$

Second, $\mathcal{D}_k(P')$ is closed. Now, suppose that $\mathcal{C}\{P\} \Downarrow n$. Since $\mathcal{C}\{P\}$ is closed, $\mathcal{C}\{P\} = \mathcal{C}\{P\}\{x_1 \leftarrow m_1\} \cdots \{x_k \leftarrow m_k\}$. Hence, by the first property of $\mathcal{D}_k$, $\mathcal{D}_k\{P\} \Downarrow n$. By the second property of $\mathcal{D}_k$, and $P \simeq P'$, $\mathcal{D}_k\{P'\} \Downarrow n$. Since $\mathcal{C}(P'')$ is closed, it follows that $\mathcal{D}_k(P'')$ is closed too. Therefore, $P' \simeq P''$ implies $\mathcal{D}_k\{P''\} \Downarrow n$. Since $\mathcal{C}\{P''\}$ is closed, $\mathcal{C}\{P''\} = \mathcal{C}\{P''\}\{x_1 \leftarrow m_1\} \cdots \{x_k \leftarrow m_k\}$. Hence, by the first property of $\mathcal{D}_k$, $\mathcal{C}\{P''\} \Downarrow n$. A symmetric argument establishes that $\mathcal{C}(P'') \Downarrow n$ implies $\mathcal{C}(P) \Downarrow n$. Hence $P \simeq P''$.

For precongruence, consider any P, Q, and $\mathcal{C}()$, with $P \simeq Q$. To show that $\mathcal{C}(P) \simeq \mathcal{C}(Q)$, consider any context $\mathcal{D}()$ and any name n with $\mathcal{D}(\mathcal{C}(P)) \Downarrow n$. Since $\mathcal{D}(\mathcal{C}())$ is a context, $P \simeq Q$ implies $\mathcal{D}(\mathcal{C}(Q)) \Downarrow n$. Similarly, $\mathcal{D}(\mathcal{C}(Q)) \Downarrow n$ implies $\mathcal{D}(\mathcal{C}(P)) \Downarrow n$. It follows that $\mathcal{C}(P) \simeq \mathcal{C}(Q)$. □

A.2 Proofs Omitted From Section 4.1

This section provides proofs of Lemma 5, Proposition 6, and Proposition 7. The main lemma of the section, Lemma 31, asserts that the hardening relation preserves structural congruence. To state and prove it, we need three auxiliary definitions.

The first auxiliary definition is a relation $P \hat{\equiv} Q$ on primes, where a *prime* is an ambient $m[P]$, an action $M.P$ where $M \in \{in\, n, out\, n, open\, n\}$, an input $(x).P$, or an output $\langle M \rangle$. The relation $P \equiv Q$ is the least to satisfy the following rules:

Structural Congruence of Primes: $P \hat{\equiv} Q$

$n[P] \hat{\equiv} n[Q]$ if $P \equiv Q$
$M.P \hat{\equiv} M.Q$ if $M \in \{in\, n, out\, n, open\, n\}$ and $P \equiv Q$
$(x).P \hat{\equiv} (x).Q$ if $P \equiv Q$
$\langle M \rangle \hat{\equiv} \langle N \rangle$ if $M = N$

This relation is clearly reflexive, symmetric, and transitive, and implies structural congruence:

Lemma 25 *For all primes P, Q, R:*

(1) $P \hat{\equiv} P$.

(2) *If $P \hat{\equiv} Q$ then $Q \hat{\equiv} P$.*

(3) *If $P \hat{\equiv} Q$ and $Q \hat{\equiv} R$ then $P \hat{\equiv} R$.*

(4) *If $P \hat{\equiv} Q$ then $P \equiv Q$.*

We prove the converse of part (4) at the end of this section.

The second auxiliary definition is a relation $C \equiv D$ on concretions:

Structural Congruence of Concretions: $C \equiv D$

$C \equiv D \quad \triangleq \quad C = (\nu\vec{r})\langle P\rangle P'$, $D = (\nu\vec{r})\langle Q\rangle Q'$, $P \mathrel{\hat{\equiv}} Q$, and $P' \equiv Q'$.

Lemma 26 *If* $C \equiv D$ *then* $\overline{(\nu n)}C \equiv \overline{(\nu n)}D$.

Proof From $C \equiv D$, it follows that $C = (\nu\vec{r})\langle P\rangle P'$, $D = (\nu\vec{r})\langle Q\rangle Q'$, $P \mathrel{\hat{\equiv}} Q$, and $P' \equiv Q'$. Now, either $n \in fn(P)$ or not. First, suppose $n \in fn(P)$.

- If $P = m[P'']$, $m \neq n$, and $n \notin fn(P')$, then $\overline{(\nu n)}C = (\nu\vec{r})\langle m[(\nu n)P'']\rangle P'$. Since $P \mathrel{\hat{\equiv}} Q$, it follows that $Q = m[Q'']$ with $P'' \equiv Q''$. By Lemma 20, $n \notin fn(P')$ implies $n \notin fn(Q')$. Therefore, $\overline{(\nu n)}D = (\nu\vec{r})\langle m[(\nu n)Q'']\rangle Q'$, and so $\overline{(\nu n)}C \equiv \overline{(\nu n)}D$.
- Otherwise, $\overline{(\nu n)}C = (\nu n, \vec{r})\langle P\rangle P'$, and $\overline{(\nu n)}D = (\nu n, \vec{r})\langle Q\rangle Q'$.

Second, if $n \notin fn(P)$, we have $n \notin fn(Q)$ by Lemma 20. Therefore, $\overline{(\nu n)}C = (\nu\vec{r})\langle P\rangle(\nu n)P'$ and $\overline{(\nu n)}D = (\nu\vec{r})\langle Q\rangle(\nu n)Q'$. □

By a similar analysis, we can prove the following:

Lemma 27 $\overline{(\nu m)(\nu n)}C \equiv \overline{(\nu n)(\nu m)}C$.

The third auxiliary definition is a relation $M > N$ on expressions, defined by the following rules:

Auxiliary Relation on Expressions: $M > N$

$M > M.\epsilon$	if $M \in \{in\, n, out\, n, open\, n\}$
$\epsilon > \epsilon$	
$M.N > M_1.(M_2.N)$	if $M > M_1.M_2$
$M.N > N'$	if $M > \epsilon$ and $N > N'$

Lemma 28 *If* $M.P > C$ *then either:*

(1) $M > M_1.M_2$, $C = (\nu)\langle M_1.R\rangle\mathbf{0}$, *and* $R \equiv M_2.P$, *or*

(2) $M > \epsilon$ *and* $P > C$.

Proof By induction on the derivation of $M.P > C$. □

Lemma 29 *If* $M > \epsilon$ *and* $P > C$ *then* $M.P > C$.

Proof By induction on the derivation of $M > \epsilon$. □

Lemma 30 *If* $M > M_1.M_2$ *then* $M.P > (\nu)\langle M_1.P'\rangle\mathbf{0}$ *with* $P' \equiv M_2.P$.

Proof By induction on the derivation of $M > M_1.M_2$. □

Next, we prove the main lemma of the section.

Lemma 31 *If $P \equiv Q$ and $Q > D$ then there is C with $P > C$ and $C \equiv D$.*

Proof We show by induction on the derivation of $P \equiv Q$, that $P \equiv Q$ implies:

(1) Whenever $P > C$ there is D with $Q > D$ and $C \equiv D$;

(2) Whenever $Q > D$ there is C with $P > C$ and $C \equiv D$.

We proceed by a case analysis of the rule that derives $P \equiv Q$.

(Struct Refl) In this case, $P = Q$. So parts (1) and (2) are trivial.

(Struct Symm) In this case, $Q \equiv P$. Part (1) follows from part (2) of the induction hypothesis, and part (2) follows from part (1) of the induction hypothesis.

(Struct Trans) In this case, $P \equiv R$ and $R \equiv Q$. For (1), suppose $P > (\nu\vec{r})\langle P_1\rangle P_2$. By induction hypothesis, $R > (\nu\vec{r})\langle R_1\rangle R_2$ with $P_1 \hat{\equiv} R_1$ and $P_2 \equiv R_2$. By induction hypothesis, again, $Q > (\nu\vec{r})\langle Q'\rangle Q''$ with $R_1 \hat{\equiv} Q_1$ and $R_2 \equiv Q_2$. By transitivity, $P_1 \hat{\equiv} Q_1$ and $P_2 \equiv Q_2$. Part (2) follows by a symmetric argument.

(Struct Res) In this case, $P = (\nu n)P'$, $Q = (\nu n)Q'$ and $P' \equiv Q'$. For (1), suppose $(\nu n)P' > C$. This can only be derived using (Harden Res), so $P' > C'$ with $C = \overline{(\nu n)}C'$. By induction hypothesis, $Q' > D'$ with $C' \equiv D'$. By (Harden Res), $Q = (\nu n)Q' > (\nu n)D'$. By Lemma 26, $\overline{(\nu n)}C' \equiv \overline{(\nu n)}D'$. Part (2) follows by a symmetric argument.

(Struct Par) In this case, $P = P' \mid R$, $Q = Q' \mid R$, and $P' \equiv Q'$. For (1), suppose $P' \mid R > (\nu\vec{r})\langle P_1\rangle P_2$. This judgment must be derived from one of the following rules:

(Harden Par 1) Here $P' > (\nu\vec{r})\langle P_1\rangle P_2'$ with $P_2 = P_2' \mid R$ and $\{\vec{r}\} \cap fn(R) = \varnothing$. By induction hypothesis, $Q' > (\nu\vec{r})\langle Q_1\rangle Q_2'$ with $P_1 \hat{\equiv} Q_1$ and $P_2' \equiv Q_2'$. Let $Q_2 = Q_2' \mid R$. By (Harden Par 1), $Q = Q' \mid R > (\nu\vec{r})\langle Q_1\rangle Q_2$. Moreover, $P_2' \mid R \equiv Q_2' \mid R$, that is, $P_2 \equiv Q_2$.

(Harden Par 2) Here $R > (\nu\vec{r})\langle P_1\rangle P_2'$ with $P_2 = P' \mid P_2'$ and $\{\vec{r}\} \cap fn(P') = \varnothing$. By Lemma 20, $fn(P') = fn(Q')$, so $\{\vec{r}\} \cap fn(Q') = \varnothing$. Let $Q_2 = Q' \mid P_2'$. By (Harden Par 2), $Q' \mid R > (\nu\vec{r})\langle P_1\rangle Q_2$. Moreover, $P' \mid P_2' \equiv Q' \mid P_2'$, that is, $P_2 \equiv Q_2$.

Part (2) follows by a symmetric argument.

(Struct Repl) In this case, $P = !P'$, $Q = !Q'$, and $P' \equiv Q'$. For (1), suppose $!P' > (\nu\vec{r})\langle P_1\rangle P_2$. This judgment must have been derived using (Harden Repl), using $P' > (\nu\vec{r})\langle P_1\rangle P_2'$, with $P_2 = P_2' \mid !P'$. By induction hypothesis, $Q' > (\nu\vec{r})\langle Q_1\rangle Q_2'$ with $P_1 \hat{\equiv} Q_1$ and $P_2' \equiv Q_2'$. Let $Q_2 = Q_2' \mid !Q'$. By (Harden Repl), $!Q' > (\nu\vec{r})\langle Q_1\rangle(Q_2' \mid !Q')$, that is, $Q > (\nu\vec{r})\langle Q_1\rangle Q_2$. Moreover, we have $P_2' \mid !P' \equiv Q_2' \mid !Q'$, that is, $P_2 \equiv Q_2$. Part (2) follows by a symmetric argument.

(Struct Amb) In this case, $P = M[P']$, $Q = M[Q']$, and $P' \equiv Q'$. For (1), suppose $M[P'] > (\nu\vec{r})\langle P_1\rangle P_2$. This judgment must have been derived using (Harden Amb), with $\vec{r} = \varnothing$, $P_1 = M[P']$, $P_2 = \mathbf{0}$, and $M = m$ for some name m. By (Harden Amb), we have $Q = m[Q'] > \langle m[Q']\rangle\mathbf{0}$. From $P' \equiv Q'$ we get $P_1 \mathrel{\hat{\equiv}} m[Q']$. Part (2) follows by a symmetric argument.

(Struct Action) In this case, $P = M.P'$, $Q = M.Q'$, and $P' \equiv Q'$. For (1), suppose $M.P' > C$ where $C = (\nu\vec{r})\langle P_1\rangle P_2$. By Lemma 28, there are two cases to consider:

- $M > M_1.M_2$, $C = \langle M_1.P''\rangle\mathbf{0}$, and $P'' \equiv M_2.P'$. By Lemma 30, $M > M_1.M_2$ implies $Q = M.Q' > \langle M_1.Q''\rangle\mathbf{0}$ where $Q'' \equiv M_2.Q'$. From $P' \equiv Q'$ it follows that $P'' \equiv Q''$ and $M_1.P'' \mathrel{\hat{\equiv}} M_1.Q''$.
- $M > \epsilon$ and $P' > C = (\nu\vec{r})\langle P_1\rangle P_2$. By induction hypothesis, $P' \equiv Q'$ and $P' > C$ imply there are Q_1, Q_2 with $Q' > (\nu\vec{r})\langle Q_1\rangle Q_2$, $P_1 \mathrel{\hat{\equiv}} Q_1$, and $P_2 \equiv Q_2$. By Lemma 29, $M > \epsilon$ and $Q' > (\nu\vec{r})\langle Q_1\rangle Q_2$ imply $Q = M.Q' > (\nu\vec{r})\langle Q_1\rangle Q_2$.

Part (2) follows by a symmetric argument.

(Struct Input) In this case, $P = (x).P'$, $Q = (x).Q'$, and $P' \equiv Q'$. For (1), suppose $P = (x).P' > C$. This can only be derived using (Harden Input), so $C = \langle (x).P'\rangle\mathbf{0}$. By (Harden Input), $Q > \langle (x).Q'\rangle\mathbf{0}$. We have $(x).P' \mathrel{\hat{\equiv}} (x).Q'$. Part (2) follows by a symmetric argument.

(Struct Par Comm) In this case, $P = R_1 \mid R_2$ and $Q = R_2 \mid R_1$. For (1), suppose $P = R_1 \mid R_2 > C$. This can only be derived using one of two rules:

(Harden Par 1) Here, $R_1 > (\nu\vec{p})\langle R_1'\rangle R_1''$ and $C = (\nu\vec{p})\langle R_1'\rangle(R_1'' \mid R_2)$ with $\{\vec{p}\} \cap fn(R_2) = \varnothing$. By (Harden Par 2), $Q = R_2 \mid R_1 > (\nu\vec{p})\langle R_1'\rangle(R_2 \mid R_1'')$. By (Struct Par Comm), $R_1'' \mid R_2 \equiv R_2 \mid R_1''$.

(Harden Par 2) This is symmetrical to the case for (Harden Par 1).

Part (2) follows by a symmetric argument.

(Struct Par Assoc) In this case, $P = (R_1 \mid R_2) \mid R_3$ and $Q = R_1 \mid (R_2 \mid R_3)$. For (1), suppose $P = (R_1 \mid R_2) \mid R_3 > C$. This can only be derived using one of two rules:

(Harden Par 1) Here, $R_1 \mid R_2 > (\nu\vec{p})\langle R'\rangle R_{12}$, $C = (\nu\vec{p})\langle R'\rangle(R_{12} \mid R_3)$, with $\{\vec{p}\} \cap fn(R_3) = \varnothing$. The judgment $R_1 \mid R_2 > (\nu\vec{p})\langle R'\rangle R_{12}$ can itself only be derived using one of two rules:

(Harden Par 1) Here, $R_1 > (\nu\vec{p})\langle R'\rangle R_1'$, and $R_{12} = R_1' \mid R_2$, with $\{\vec{p}\} \cap fn(R_2) = \varnothing$. We have $\{\vec{p}\} \cap fn(R_2 \mid R_3) = \varnothing$. Hence, by (Harden Par 1), $R_1 > (\nu\vec{p})\langle R'\rangle R_1'$ implies $Q = R_1 \mid (R_2 \mid R_3) > (\nu\vec{p})\langle R'\rangle(R_1' \mid (R_2 \mid R_3))$. Moreover, $R_{12} \mid R_3 = (R_1' \mid R_2) \mid R_3 \equiv R_1' \mid (R_2 \mid R_3)$.

(Harden Par 2) Here $R_2 > (\nu\vec{p})\langle R'\rangle R_2'$, $R_{12} = R_1 \mid R_2'$, with $\{\vec{p}\} \cap \mathit{fn}(R_1) = \varnothing$. By (Harden Par 1), $R_2 > (\nu\vec{p})\langle R'\rangle R_2'$ and $\{\vec{p}\} \cap \mathit{fn}(R_3) = \varnothing$ imply $R_2 \mid R_3 > (\nu\vec{p})\langle R'\rangle(R_2' \mid R_3)$. By (Harden Par 1), this and $\{\vec{p}\} \cap \mathit{fn}(R_1) = \varnothing$ imply $Q = R_1 \mid (R_2 \mid R_3) > (\nu\vec{p})\langle R'\rangle(R_1 \mid (R_2' \mid R_3))$. Moreover, $R_{12} \mid R_3 = (R_1 \mid R_2') \mid R_3 \equiv R_1 \mid (R_2' \mid R_3)$.

(Harden Par 2) This is symmetrical to the case for (Harden Par 1).

Part (2) follows by a symmetric argument.

(Struct Repl Par) In this case, $P = !P'$ and $Q = P' \mid !P'$.

For (1), suppose $P = !P' > (\nu\vec{r})\langle P_1\rangle P_2$. This can only have been derived using (Harden Repl), from $P' > (\nu\vec{r})\langle P_1\rangle P_2'$ with $P_2 = P_2' \mid !P'$. By Lemma 22, $\mathit{fn}(!P') = \mathit{fn}((\nu\vec{r})\langle P_1\rangle P_2)$. Therefore, $\{\vec{r}\} \cap \mathit{fn}(P') = \varnothing$. Let $Q_2 = P' \mid P_2$. By (Harden Par 1), $!P' > (\nu\vec{r})\langle P_1\rangle P_2$ implies $P' \mid !P' > (\nu\vec{r})\langle P_1\rangle(P' \mid P_2)$, that is, $Q > (\nu\vec{r})\langle P_1\rangle Q_2$. We have $P_2 = P_2' \mid !P' \equiv P' \mid (P_2' \mid !P') \equiv P' \mid P_2 \equiv Q_2$. For (2), suppose $Q = P' \mid !P' > (\nu\vec{r})\langle Q_1\rangle Q_2$. This must have been derived using one of the following two rules:

(Harden Par 1) Here, $P' > (\nu\vec{r})\langle Q_1\rangle Q_2'$ with $Q_2 = Q_2' \mid !P'$ and $\{\vec{r}\} \cap \mathit{fn}(!P') = \varnothing$. By (Harden Repl), $P = !P' > (\nu\vec{r})\langle Q_1\rangle Q_2$.

(Harden Par 2) Here, $!P' > (\nu\vec{r})\langle Q_1\rangle Q_2'$ with $Q_2 = P' \mid Q_2'$ and $\{\vec{r}\} \cap \mathit{fn}(P') = \varnothing$. The judgment $!P' > (\nu\vec{r})\langle Q_1\rangle Q_2'$ can only have been derived with (Harden Repl). Therefore, $P > (\nu\vec{r})\langle Q_1\rangle Q_2''$ with $Q_2' = Q_2'' \mid !P'$. Hence, $Q_2' \equiv Q_2'' \mid !P' \mid P' \equiv P' \mid Q_2' = Q_2$.

(Struct Res Res) In this case, $P = (\nu n)(\nu m)R$ and $Q = (\nu m)(\nu n)R$. We assume that $m \neq n$; if $m = n$ the case is trivial. For (1), suppose $P > C$. This can only be derived using (Harden Res), twice, with $R > C'$ and $C = \overline{(\nu n)(\nu m)}C'$. By (Harden Res), twice, we get $Q > (\nu m)(\nu n)C'$. By Lemma 27, $C \equiv \overline{(\nu m)(\nu n)}C'$. Part (2) follows by a symmetric argument.

(Struct Res Par) In this case, $P = (\nu n)(R_1 \mid R_2)$, $Q = R_1 \mid (\nu n)R_2$, and $n \notin \mathit{fn}(R_1)$. For (1), suppose $P > C$. This can only have been derived using (Harden Res), with $C = \overline{(\nu n)}C'$ and $R_1 \mid R_2 > C'$ with $C' = (\nu\vec{r})\langle R'\rangle R_{12}$. Since the names $\vec{r}$ are bound, we may assume that $n \notin \{\vec{r}\}$. We examine the ways in which the restricted concretion $\overline{(\nu n)}C'$ may be defined.

- Here $n \in \mathit{fn}(R')$. The judgment $R_1 \mid R_2 > (\nu\vec{r})\langle R'\rangle R_{12}$ may be derived in one of two ways:

  (Harden Par 1) Then $R_1 > (\nu\vec{r})\langle R'\rangle R_1'$ and $R_{12} = R_1' \mid R_2$ with $\{\vec{r}\} \cap \mathit{fn}(R_2) = \varnothing$. By Lemma 22, $R_1 > (\nu\vec{r})\langle R'\rangle R_1'$ implies $\mathit{fn}(R_1) = \mathit{fn}((\nu\vec{r})\langle R'\rangle R_1')$, that is, $\mathit{fn}(R_1) = (\mathit{fn}(R') \cup \mathit{fn}(R_1')) - \{\vec{r}\}$. From this we obtain a contradiction, since we have that $n \notin \mathit{fn}(R_1)$ yet also that $n \in \mathit{fn}(R')$, with $n \notin \{\vec{r}\}$. So this case cannot arise.

(Harden Par 2) Then $R_2 > (\nu\vec{r})\langle R'\rangle R_2'$ and $R_{12} = R_1 \mid R_2'$ with $\{\vec{r}\} \cap fn(R_1) = \varnothing$.

In subcase (a), $R' = m[R'']$, $m \neq n$, $n \notin fn(R_{12})$, that is, $n \notin fn(R_1) \cup fn(R_2')$, and $C = (\nu\vec{r})\langle m[(\nu n)R'']\rangle(R_1 \mid R_2')$. By (Harden Res), $(\nu n)R_2 > (\nu\vec{r})\langle m[(\nu n)R'']\rangle R_2'$. By (Harden Par 2), we have $R_1 \mid (\nu n)R_2 > (\nu\vec{r})\langle m[(\nu n)R'']\rangle(R_1 \mid R_2')$.

Otherwise, subcase (b), $C = (\nu n, \vec{r})\langle R'\rangle R_{12}$. By (Harden Res), we have $(\nu n)R_2 > (\nu n, \vec{r})\langle R'\rangle R_2'$. By (Harden Par 2), $n \notin fn(R_1)$ implies $R_1 \mid (\nu n)R_2 > (\nu n, \vec{r})\langle R'\rangle(R_1 \mid R_2')$. Moreover, $R_{12} = R_1 \mid R_2'$.

- Here $n \notin fn(R')$. The judgment $R_1 \mid R_2 > (\nu\vec{r})\langle R'\rangle R_{12}$ may be derived in one of two ways:

  (Harden Par 1) Then $R_1 > (\nu\vec{r})\langle R'\rangle R_1'$ and $R_{12} = R_1' \mid R_2$ with $\{\vec{r}\} \cap fn(R_2) = \varnothing$. From $\{\vec{r}\} \cap fn(R_2) = \varnothing$ it follows that $\{\vec{r}\} \cap fn((\nu n)R_2) = \varnothing$. Hence, by (Harden Par 1), $Q = R_1 \mid (\nu n)R_2 > (\nu\vec{r})\langle R'\rangle(R_1' \mid (\nu n)R_2)$. By Lemma 22, $R_1 > (\nu\vec{r})\langle R'\rangle R_1'$ implies $fn(R_1) = fn((\nu\vec{r})\langle R'\rangle R_1')$, that is, $fn(R_1) = (fn(R') \cup fn(R_1')) - \{\vec{r}\}$. Since $n \notin \{\vec{r}\}$ and $n \notin fn(R_1)$, it follows that $n \notin fn(R_1')$. Hence, we have $(\nu n)R_{12} = (\nu n)(R_1' \mid R_2) \equiv R_1' \mid (\nu n)R_2$.

  (Harden Par 2) Then $R_2 > (\nu\vec{r})\langle R'\rangle R_2'$ and $R_{12} = R_1 \mid R_2'$ with $\{\vec{r}\} \cap fn(R_1) = \varnothing$. By (Harden Res), $n \notin \{\vec{r}\} \cup fn(R')$ implies $(\nu n)R_2 > (\nu\vec{r})\langle R'\rangle(\nu n)R_2'$. By (Harden Par 2), $Q = R_1 \mid (\nu n)R_2 > (\nu\vec{r})\langle R'\rangle(R_1 \mid (\nu n)R_2')$. Since $n \notin fn(R_1)$, we have $(\nu n)R_{12} = (\nu n)(R_1 \mid R_2') \equiv R_1 \mid (\nu n)R_2'$.

Part (2) follows by a similar, though not precisely symmetrical, argument.

(Struct Res Amb) In this case, $P = (\nu n)m[R]$, $Q = m[(\nu n)R]$, and $n \neq m$. For (1), suppose $P > C$. This can only have been derived using (Harden Res), with $m[R] > D$ and $C = (\nu n)D$. The judgment $m[R] > D$ may only be derived using (Harden Amb), so $D = (\nu)\langle m[R]\rangle\mathbf{0}$. Since $C = (\nu n)(\nu)\langle m[R]\rangle\mathbf{0}$, there are two cases to consider, depending on whether $n \in fn(R)$:

- Suppose $n \in fn(R)$. Then $C = (\nu)\langle m[(\nu n)R]\rangle\mathbf{0}$. By (Harden Amb), $Q > (\nu)\langle m[(\nu n)R]\rangle\mathbf{0}$.
- Suppose $n \notin fn(R)$. Then $C = (\nu)\langle m[R]\rangle(\nu n)\mathbf{0}$. By (Harden Amb), $Q > (\nu)\langle m[(\nu n)R]\rangle\mathbf{0}$. By Lemma 24, we have $m[R] \mathrel{\hat{\equiv}} m[(\nu n)R]$, and by (Struct Zero Res), we have $(\nu n)\mathbf{0} \equiv \mathbf{0}$.

For (2), suppose $Q > C$. This can only have been derived using (Harden Amb), so $C = (\nu)\langle m[(\nu n)R]\rangle\mathbf{0}$. We proceed by cases depending on whether $n \in fn(R)$.

- Suppose $n \in fn(R)$. Then $P = (\nu n)m[R] > (\nu)\langle m[(\nu n)R]\rangle\mathbf{0}$.

- Suppose $n \notin fn(R)$. Then $P = (\nu n)m[R] > (\nu)\langle m[R]\rangle(\nu n)\mathbf{0}$. By Lemma 24, we have $m[R] \hat{\equiv} m[(\nu n)R]$, and by (Struct Zero Res), we have $(\nu n)\mathbf{0} \equiv \mathbf{0}$.

(Struct Zero Par) In this case, $P = Q \mid \mathbf{0}$. For (1), suppose $P > C$. This can only have been derived using one of two rules:

(Harden Par 1) Here, $Q > (\nu\vec{q})\langle Q'\rangle Q''$ and $C = (\nu\vec{q})\langle Q'\rangle(Q'' \mid \mathbf{0})$. Since $Q'' \mid \mathbf{0} \equiv Q''$, we are done.

(Harden Par 2) For this rule to be applicable, we would need a hardening $\mathbf{0} > C$, but no rule can derive $\mathbf{0} > C$ for any C.

For (2), suppose $Q > (\nu\vec{q})\langle Q'\rangle Q''$. By (Harden Par 2), $P = Q \mid \mathbf{0} > (\nu\vec{q})\langle Q'\rangle(Q'' \mid \mathbf{0})$. Moreover, $Q'' \mid \mathbf{0} \equiv Q''$.

(Struct Zero Res) In this case, $P = (\nu n)\mathbf{0}$ and $Q = \mathbf{0}$. Parts (1) and (2) hold vacuously, since no hardening $P > C$ or $Q > C$ are derivable.

(Struct Zero Repl) In this case, $P = !\mathbf{0}$ and $Q = \mathbf{0}$. Again, parts (1) and (2) hold vacuously, since no hardening $P > C$ or $Q > C$ are derivable.

(Struct ϵ) Here, $P = \epsilon.Q$. For (1), suppose $P = \epsilon.Q > C$. Only (Harden ϵ) can derive this, with $Q > C$. For (2), suppose $Q > C$. By (Harden ϵ), $P = \epsilon.Q > C$.

(Struct .) Here, $P = (M.M').R$ and $Q = M.(M'.R)$.

For (1), suppose $P = (M.M').R > C$. Only (Harden .) can derive this, with $M.(M'.R) > C$, that is, $Q > C$.

For (2), suppose $Q = M.(M'.R) > C$. By Lemma 28, one of two cases holds:

- $M > M_1.M_2$, $C = \langle M_1.R'\rangle\mathbf{0}$, and $R' \equiv M_2.(M'.R)$. By Lemma 30, $M > M_1.M_2$ implies that $Q = M.(M'.R) > \langle M_1.R''\rangle\mathbf{0}$ with $R'' \equiv M_2.(M'.R)$. By (Harden .), this implies $P = (M.M').R > \langle M_1.R'\rangle\mathbf{0}$. Moreover, $M_1.R' \equiv M_1.(M_2.(M'.R)) \equiv M_1.R''$.
- $M > \epsilon$ and $M'.R > C$. By Lemma 29, $M > \epsilon$ implies $M.M'.R > C$. By (Harden .), this implies $P = (M.M').R > C$. □

We can now prove three facts stated in Section 4.1.

Proof of Lemma 5 *If $P > (\nu\vec{p})\langle P'\rangle P''$ then $P \equiv (\nu\vec{p})(P' \mid P'')$.*

Proof By induction on the derivation of $P > (\nu\vec{p})\langle P'\rangle P''$. We consider just one case in detail. The other cases are no harder.

(Harden Repl) Here, $!P > (\nu\vec{p})\langle P'\rangle(P'' \mid !P)$ follows from $P > (\nu\vec{p})\langle P'\rangle P''$. By induction hypothesis, $P \equiv (\nu\vec{p})(P' \mid P'')$. By Lemma 20, $fn(P) = fn((\nu\vec{p})(P' \mid P''))$, and therefore, $\{\vec{p}\} \cap fn(P) = \varnothing$. Hence, we get: $!P \equiv P \mid !P \equiv (\nu\vec{p})(P' \mid P'') \mid !P \equiv (\nu\vec{p})(P' \mid P'' \mid !P)$. □

Proof of Proposition 6 *If $P \equiv Q$ and $Q > (\nu\vec{r})\langle Q'\rangle Q''$ then there are P' and P'' with $P > (\nu\vec{r})\langle P'\rangle P''$, $P' \equiv Q'$, and $P'' \equiv Q''$.*

Proof Combine Lemma 25 and Lemma 31. □

Proof of Proposition 7 *$P \downarrow n$ if and only if there exist $\vec{p}$, P', P'' such that $P > (\nu\vec{p})\langle n[P']\rangle P''$ and $n \notin \{\vec{p}\}$.*

Proof First, suppose $P \downarrow n$, that is, there are $\vec{p}$, R', R'' with $n \notin \{\vec{p}\}$ and $P \equiv R$ where $R = (\nu\vec{p})(n[R'] \mid R'')$. Given (Struct Res Amb) and (Struct Res Par), we may assume that $\{\vec{p}\} \subseteq \mathit{fn}(R') \cap \mathit{fn}(R'')$. Therefore, we may derive $R > (\nu\vec{r})\langle n[R']\rangle(\mathbf{0} \mid R'')$. By Lemma 31, $P \equiv R$ implies there are P', P'' such that $P > (\nu\vec{r})\langle n[P']\rangle P''$, $P' \equiv R'$, and $P'' \equiv R''$.

Second, suppose $P > (\nu\vec{p})\langle n[P']\rangle P''$ and $n \notin \{\vec{p}\}$. By Lemma 5, $P \equiv (\nu\vec{p})(n[P'] \mid P'')$. Therefore, $P \downarrow n$. □

We end this section by exploring another consequence of Lemma 31.

Proposition 32 *For all primes P and Q, if $P \equiv Q$, then $P \mathrel{\hat{\equiv}} Q$.*

Proof Since P and Q are primes, their only hardenings are $P > (\nu)\langle P\rangle\mathbf{0}$ and $Q > (\nu)\langle Q\rangle\mathbf{0}$. By Lemma 31, $P \mathrel{\hat{\equiv}} Q$. □

A corollary of Lemma 25 and Proposition 32 is that for all primes P and Q, $P \equiv Q$ if and only if $P \mathrel{\hat{\equiv}} Q$. For example, it follows that $m[P] \equiv n[Q]$ if and only if $m = n$ and $P \equiv Q$.

A.3 Proofs Omitted From Section 4.2

This section provides a proof of Theorem 9, that $P \rightarrow Q$ if and only if there is R with $P \xrightarrow{\tau} R$ and $R \equiv Q$. We prove each direction separately, starting with the right-to-left implication.

First, we need the following lemma:

Lemma 33 *If $P \xrightarrow{M} P'$ then $P \equiv (\nu\vec{p})(P_1 \mid M.P_2)$ with $P' \equiv (\nu\vec{p})(P_1 \mid P_2)$ and $\mathit{fn}(M) \cap \{\vec{p}\} = \varnothing$.*

Proof Only (Trans Cap) may derive the judgment $P \xrightarrow{M} P'$. So we have $P > (\nu\vec{p})\langle M.P_1\rangle P_2$, $P' = (\nu\vec{p})(P_1 \mid P_2)$, $M \in \{\mathit{in}\,n, \mathit{out}\,n, \mathit{open}\,n\}$, and $n \notin \{\vec{p}\}$. By Proposition 5, $P \equiv (\nu\vec{p})(M.P_1 \mid P_2)$. Moreover, $\mathit{fn}(M) = \{n\}$, so the result follows. □

We use the following to establish the right-to-left direction of Theorem 9.

Proposition 34 *If $P \xrightarrow{\tau} P'$ then $P \rightarrow P'$.*

Proof By induction on the derivation of $P \xrightarrow{\tau} P'$. We examine one case:

(Trans In) We have $P > (\nu\vec{p})\langle n[Q]\rangle R$, $Q \xrightarrow{in\, m} Q'$, $R > (\nu\vec{r})\langle m[R']\rangle R''$, and $P' = (\nu\vec{p},\vec{r})(m[n[Q'] \mid R'] \mid R'')$ with $\{\vec{r}\} \cap fn(n[Q]) = \varnothing$. By Lemma 5, $P \equiv (\nu\vec{p})(n[Q] \mid R)$. By Lemma 33, $Q \equiv (\nu\vec{q})(Q_1 \mid in\, n.Q_2)$, with $Q' \equiv (\nu\vec{q})(Q_1 \mid Q_2)$ and $n \notin \{\vec{q}\}$. Since the names $\vec{q}$ are bound, we may assume that $\{\vec{q}\} \cap fn(m[R']) = \varnothing$. By Lemma 5, $R \equiv (\nu\vec{r})(m[R'] \mid R'')$. Hence, we have:

$$\begin{array}{rcl} P & \equiv & (\nu\vec{p})(n[(\nu\vec{q})(Q_1 \mid in\, n.Q_2)] \mid (\nu\vec{r})(m[R'] \mid R'')) \\ & \equiv & (\nu\vec{p},\vec{r})((\nu\vec{q})(n[Q_1 \mid in\, n.Q_2] \mid m[R']) \mid R'') \\ & \rightarrow & (\nu\vec{p},\vec{r})((\nu\vec{q})(m[n[Q_1 \mid Q_2] \mid R']) \mid R'') \\ & \equiv & (\nu\vec{p},\vec{r})(m[n[Q'] \mid R'] \mid R'') \\ & = & P' \end{array}$$

The other cases follow similarly. □

Next, we prove a couple of lemmas needed for proving the left-to-right direction of Theorem 9.

Lemma 35 *If $P \equiv Q$ and $Q \xrightarrow{\alpha} Q'$ then there is P' such that $P \xrightarrow{\alpha} P'$ and $P' \equiv Q'$.*

Proof By induction on the derivation of $Q \xrightarrow{\alpha} Q'$.

(Trans Cap) We have $Q > (\nu\vec{r})\langle M.Q_1\rangle Q_2$ with $Q' = (\nu\vec{r})(Q_1 \mid Q_2)$, $M \in \{in\ n, out\ n, open\ n\}$, and $n \notin \{\vec{r}\}$. By Lemma 31, there are P_1 and P_2 with $P > (\nu\vec{r})\langle M.P_1\rangle P_2$, $P_1 \equiv Q_1$, and $P_2 \equiv Q_2$. By (Trans Cap), $P \xrightarrow{M} (\nu\vec{r})(P_1 \mid P_2)$, and we have that $(\nu\vec{r})(P_1 \mid P_2) \equiv Q'$.

(Trans In) We have $Q > (\nu\vec{q})\langle n[Q_1]\rangle Q_2$, $Q_1 \xrightarrow{in\, m} Q_1'$, $Q_2 > (\nu\vec{r})\langle m[Q_2']\rangle Q_2''$, and $Q' = (\nu\vec{q},\vec{r})(m[n[Q_1'] \mid Q_2'] \mid Q_2'')$ with $\{\vec{r}\} \cap fn(n[Q_1]) = \varnothing$. By Lemma 31, $P > (\nu\vec{q})\langle n[P_1]\rangle P_2$, with $P_1 \equiv Q_1$ and $P_2 \equiv Q_2$. By induction hypothesis, $P_1 \xrightarrow{in\, m} P_1'$ with $P_1' \equiv Q_1'$. By Lemma 31, $P_2 > (\nu\vec{r})\langle m[P_2']\rangle P_2''$, with $P_2' \equiv Q_2'$ and $P_2'' \equiv Q_2''$. By Lemma 20, $fn(n[P_1]) = fn(n[Q_1])$, and therefore $\{\vec{r}\} \cap fn(n[P_1]) = \varnothing$. Let $P' = (\nu\vec{q},\vec{r})(m[n[P_1'] \mid P_2'] \mid P_2'')$. By (Trans In), we have $P \xrightarrow{\tau} P'$. Moreover, $P' \equiv (\nu\vec{q},\vec{r})(m[n[Q_1'] \mid Q_2'] \mid Q_2'')$, that is, $P' \equiv Q'$.

(Trans Out) We have $Q > (\nu\vec{p})\langle n[Q_1]\rangle Q_2$, $Q_1 > (\nu\vec{q})\langle m[Q_3]\rangle Q_4$, and $Q_3 \xrightarrow{out\, n} Q_3'$, with $Q' = (\nu\vec{p})(Q_2 \mid (\nu\vec{q})(n[Q_4] \mid m[Q_3']))$ and $n \notin \{\vec{q}\}$. By Lemma 31, $P > (\nu\vec{p})\langle n[P_1]\rangle P_2$, with $P_1 \equiv Q_1$ and $P_2 \equiv Q_2$. By Lemma 31, $P_1 > (\nu\vec{q})\langle m[P_3]\rangle P_4$, with $P_3 \equiv Q_3$ and $P_4 \equiv Q_4$. By induction hypothesis, $P_3 \xrightarrow{out\, n} P_3'$ with $P_3' \equiv Q_3'$. Let $P' = (\nu\vec{p})(P_2 \mid (\nu\vec{q})(n[P_4] \mid m[P_3']))$. By (Trans Out), we have $P \xrightarrow{\tau} P'$. Moreover, $P' \equiv (\nu\vec{p})(Q_2 \mid (\nu\vec{q})(n[Q_4] \mid m[Q_3']))$, that is, $P' \equiv Q'$.

(Trans Amb) We have $Q > (\nu\vec{r})\langle n[Q_1]\rangle Q_2$, $Q_1 \xrightarrow{\tau} Q'_1$, $Q' = (\nu\vec{r})\langle n[Q'_1]\rangle Q_2$. By Lemma 31, $P > (\nu\vec{r})\langle n[P_1]\rangle P_2$ with $P_1 \equiv Q_1$ and $P_2 \equiv Q_2$. By induction hypothesis, $P_1 \xrightarrow{\tau} P'_1$ with $P'_1 \equiv Q'_1$. Let $P' = (\nu\vec{r})\langle n[P'_1]\rangle P_2$. By (Trans Amb), $P \xrightarrow{\tau} P'$. Moreover, $P' \equiv (\nu\vec{r})\langle n[Q'_1]\rangle Q_2$, that is, $P' \equiv Q'$.

The other cases, (Trans Open) and (Trans I/O), follow similarly. □

Lemma 36

(1) *If $P \xrightarrow{\alpha} P'$ and $n \notin fn(\alpha)$ there is Q with $(\nu n)P \xrightarrow{\alpha} Q$ and $Q \equiv (\nu n)P'$.*

(2) *If $(\nu n)P \xrightarrow{\alpha} Q$ then $n \notin fn(\alpha)$ there is P' with $P \xrightarrow{\alpha} P'$ and $Q \equiv (\nu n)P'$.*

Proof By inductions on the derivations of $P \xrightarrow{\alpha} P'$ and $(\nu n)P \xrightarrow{\alpha} Q$ respectively. We omit the details. □

The following establishes the left-to-right direction of Theorem 9.

Proposition 37 *If $P \rightarrow Q$ then $P \xrightarrow{\tau}\equiv Q$.*

Proof By induction on the derivation of $P \rightarrow Q$.

(Red In) $P = n[in\ m.P_1 \mid P_2] \mid m[P_3]$ and $Q = m[n[P_1 \mid P_2] \mid P_3]$. We can easily calculate that $P \xrightarrow{\tau}\equiv Q$.

(Red Out) $P = m[n[out\ m.P_1 \mid P_2] \mid P_3]$ and $Q = n[P_1 \mid P_2] \mid m[P_3]$. We can easily calculate that $P \xrightarrow{\tau}\equiv Q$.

(Red Open) $P = open\ n.P_1 \mid n[P_2]$ and $Q = P_1 \mid P_2$. We can easily calculate that $P \xrightarrow{\tau}\equiv Q$.

(Red I/O) $P = \langle M\rangle \mid (x).P_1$ and $Q = P_1\{x{\leftarrow}M\}$. We can easily calculate that $P \xrightarrow{\tau}\equiv Q$.

(Red Par) $P = P_1 \mid P_2$ and $Q = P'_1 \mid P_2$ with $P_1 \rightarrow P'_1$. By induction hypothesis, there is R with $P_1 \xrightarrow{\tau} R$ and $R \equiv P'_1$. By a case analysis of the derivation of $P_1 \xrightarrow{\tau} R$, we can show that $P_1 \mid P_2 \xrightarrow{\tau}\equiv R \mid P_2$. Hence, $P_1 \mid P_2 \xrightarrow{\tau}\equiv P'_1 \mid P_2$.

(Red Res) $P = (\nu n)P_1$ and $Q = (\nu n)P'_1$ with $P_1 \rightarrow P'_1$. By induction hypothesis, there is R with $P_1 \xrightarrow{\tau} R$ and $R \equiv P'_1$. By Lemma 36, $P_1 \xrightarrow{\tau} R$, implies that $(\nu n)P_1 \xrightarrow{\tau}\equiv (\nu n)R$. Hence, $(\nu n)P_1 \xrightarrow{\tau}\equiv (\nu n)P'_1$.

(Red Amb) $P = n[P']$, $Q = n[P'_1]$ with $P_1 \rightarrow P'_1$. By induction hypothesis, there is R with $P_1 \xrightarrow{\tau} R$ and $R \equiv P'_1$. By (Trans Amb), we get that $n[P'] \xrightarrow{\tau} n[R] \mid \mathbf{0}$. Hence, $n[P'] \xrightarrow{\tau}\equiv n[P'_1]$.

(Red $\equiv$) Here, $P \equiv P'$, $P' \rightarrow Q'$, and $Q' \equiv Q$. By induction hypothesis, $P' \xrightarrow{\tau}\equiv Q'$. By (Struct Trans), this and $Q' \equiv Q$ imply $P' \xrightarrow{\tau}\equiv Q$. By Lemma 35, $P \equiv P'$ and $P' \xrightarrow{\tau}\equiv Q$ imply that $P \xrightarrow{\tau}\equiv Q$. □

Proof of Theorem 9 *$P \rightarrow Q$ if and only if $P \xrightarrow{\tau}\equiv Q$.*

Proof Combine Proposition 34, Proposition 37, and rule (Red $\equiv$). □

A.4 Proofs Omitted From Section 4.4

We provide proofs for Lemma 13 and Theorem 15.

Proof of Lemma 13 *If $H\{P\} > (\nu\vec{p})\langle P_1\rangle P_2$ then either:*

(1) *$H > (\nu\vec{p})\langle n[H']\rangle P_2$ and $P_1 = n[H'\{P\}]$, or*

(2) *$H > (\nu\vec{p})\langle P_1\rangle H'$ and $P_2 = H'\{P\}$, or*

(3) *$P > (\nu\vec{p})\langle P_1\rangle P'$, $H \equiv - \mid R$, $P_2 \equiv P' \mid R$, and $\{\vec{p}\} \cap fn(R) = \varnothing$.*

Proof By induction on the derivation of $H\{P\} > (\nu\vec{p})\langle P_1\rangle P_2$.

(Harden Action) Then $H\{P\} = M.Q$ and $(\nu\vec{p})\langle P_1\rangle P_2 = (\nu)\langle M.Q\rangle\mathbf{0}$ with $M \in \{\mathit{in}\ n, \mathit{out}\ n, \mathit{open}\ n\}$. Since $M.Q$ cannot be a harness, it must be that $H = -$. So $P = M.Q > (\nu)\langle M.Q\rangle\mathbf{0}$. Case (3) of the lemma pertains, with $R = \mathbf{0}$.

(Harden ϵ) Then $H\{P\} = \epsilon.Q$ and $Q > (\nu\vec{p})\langle P_1\rangle P_2$. Since $\epsilon.Q$ cannot be a harness, it must be that $H = -$, and $P = \epsilon.Q > (\nu\vec{p})\langle P_1\rangle P_2$. Case (3) of the lemma pertains, with $R = \mathbf{0}$.

(Harden .) Then $H\{P\} = (M.N).Q$ and $M.(N.Q) > (\nu\vec{p})\langle P_1\rangle P_2$. Since $(M.N).Q$ cannot be a harness, we must have $H = -$ and $P = (M.N).Q > (\nu\vec{p})\langle P_1\rangle P_2$. Case (3) of the lemma pertains, with $R = \mathbf{0}$.

(Harden Amb) Then $H\{P\} = n[Q]$ and $(\nu\vec{p})\langle P_1\rangle P_2 = (\nu)\langle n[Q]\rangle\mathbf{0}$. There are two cases to consider: either $H = -$ and $P = n[Q]$, or $H = n[H']$ and $Q = H'\{P\}$. In the first case, we have that $P > (\nu\vec{p})\langle P_1\rangle P_2$. So case (3) of the lemma pertains, with $R = \mathbf{0}$. In the second case, we have that $H > (\nu)\langle n[H']\rangle\mathbf{0} = (\nu\vec{p})\langle n[H']\rangle P_2$, and $P_1 = n[Q] = n[H'\{P\}]$. So case (1) of the lemma pertains.

(Harden Input) Then $H\{P\} = (x).Q$ and $(\nu\vec{p})\langle P_1\rangle P_2 = (\nu)\langle (x).Q\rangle\mathbf{0}$. Since $(x).Q$ cannot be a harness, it must be that $H = -$. So $P = (x).Q > (\nu)\langle (x).Q\rangle\mathbf{0}$. Case (3) of the lemma pertains, with $R = \mathbf{0}$.

(Harden Output) Then $H\{P\} = \langle M\rangle$ and $(\nu\vec{p})\langle P_1\rangle P_2 = (\nu)\langle\langle M\rangle\rangle\mathbf{0}$. Since $\langle M\rangle$ cannot be a harness, it must be that $H = -$. So $P = \langle M\rangle > (\nu)\langle\langle M\rangle\rangle\mathbf{0}$. Case (3) of the lemma pertains, with $R = \mathbf{0}$.

(Harden Par 1) Then $H\{P\} = Q_1 \mid Q_2$, $Q_1 > (\nu\vec{p})\langle P_1\rangle P_3$, and $P_2 = P_3 \mid Q_2$, with $\{\vec{p}\} \cap fn(Q_2) = \varnothing$. Given that $H\{P\} = Q_1 \mid Q_2$, there are three cases to consider:

- Here $H = -$ and $P = Q_1 \mid Q_2$. Case (3) of the lemma pertains, with $R = \mathbf{0}$.
- Here $H = Q_1 \mid H_2$ and $Q_2 = H_2\{P\}$. By (Harden Par 1) and $\{\vec{p}\} \cap fn(Q_2) = \varnothing$, we may derive $H\{R\} > (\nu\vec{p})\langle P_1\rangle(P_3 \mid H_2\{R\})$ for all R with $\{\vec{p}\} \cap fn(R) = \varnothing$. Let $H' = P_3 \mid H_2$. We have $H > (\nu\vec{p})\langle P_1\rangle H'$, and moreover, $P_2 = P_3 \mid Q_2 = P_3 \mid H_2\{P\} = H'\{P\}$. So case (2) of the lemma pertains.
- Here $H = H_1 \mid Q_2$ and $Q_1 = H_1\{P\}$. By induction hypothesis, $H_1\{P\} > (\nu\vec{p})\langle P_1\rangle P_3$ implies that one of three cases holds:
  (1) $H_1 > (\nu\vec{p})\langle n[H']\rangle P_3$ and $P_1 = n[H'\{P\}]$. We can derive $H > (\nu\vec{p})\langle n[H']\rangle(P_3 \mid Q_2)$ since $\{\vec{p}\} \cap fn(Q_2) = \varnothing$. Therefore, $H > (\nu\vec{p})\langle n[H']\rangle P_2$, as required to establish case (1) of the lemma.
  (2) $H_1 > (\nu\vec{p})\langle P_1\rangle H'$ and $P_3 = H'\{P\}$. We have $H > (\nu\vec{p})\langle P_1\rangle(H' \mid Q_2)$ since $\{\vec{p}\} \cap fn(Q_2) = \varnothing$. Moreover, $P_2 = P_3 \mid Q_2 = H'\{P\} \mid Q_2$. This establishes case (2) of the lemma.
  (3) $P > (\nu\vec{p})\langle P_1\rangle P'$, $H_1 \equiv - \mid R$, $P_3 \equiv P' \mid R$, and $\{\vec{p}\} \cap fn(R) = \varnothing$. We have $H \equiv - \mid R \mid Q_2$, $P_2 \equiv P' \mid R \mid Q_2$, and $\{\vec{p}\} \cap fn(R \mid Q_2) = \varnothing$. This establishes case (3) of the lemma.

(Harden Par 2) Similar to the case for (Harden Par 1).

(Harden Repl) Then $H\{P\} = !Q > (\nu\vec{p})\langle P_1\rangle P_2$, $Q > (\nu\vec{p})\langle P_1\rangle Q'$, and $P_2 = Q' \mid !Q$. Given that a replication cannot be a harness, $H\{P\} = !Q$ implies that $H = -$ and $P = !Q$. Let $R = \mathbf{0}$, and we have $P > (\nu\vec{p})\langle P_1\rangle P_2$, $H \equiv - \mid R$, $P_2 \equiv P_2 \mid R$, and $\{\vec{p}\} \cap fn(R) = \varnothing$. Therefore, case (3) of the lemma pertains.

(Harden Res) Then $H\{P\} = (\nu m)Q$, $Q > (\nu\vec{q})\langle Q_1\rangle Q_2$, and $(\nu\vec{p})\langle P_1\rangle P_2 = \overline{(\nu m)}(\nu\vec{q})\langle Q_1\rangle Q_2$. From $H\{P\} = (\nu m)Q$, it follows that $m \notin fn(P)$ since $fn(P) \subseteq fn(H\{P\})$. Since the name m is bound, we may assume that $m \notin fn(P)$, and also that $m \notin \{\vec{q}\}$. Given that $H\{P\} = (\nu m)Q$, there are two cases to consider. In the first, $H = -$ and $P = (\nu m)Q$, so case (3) of the lemma pertains, with $R = \mathbf{0}$. In the second, $H = (\nu m)H_1$ and $Q = H_1\{P\}$. We examine the three cases in the definition of $\overline{(\nu m)}(\nu\vec{q})\langle Q_1\rangle Q_2$.

- Here $Q_1 = q[Q_1']$ with $m \in fn(Q_1')$ but $m \neq q$, and $m \notin fn(Q_2)$, so that:

$$\begin{array}{rcl} \overline{(\nu m)}(\nu\vec{q})\langle Q_1\rangle Q_2 & = & (\nu\vec{q})\langle q[(\nu m)Q_1']\rangle Q_2 \\ & = & (\nu\vec{p})\langle P_1\rangle P_2 \end{array}$$

  Therefore, $\vec{p} = \vec{q}$, $P_1 = q[(\nu m)Q_1']$, and $P_2 = Q_2$. We have that:

$$H_1\{P\} = Q > (\nu\vec{q})\langle Q_1\rangle Q_2 = (\nu\vec{p})\langle q[Q_1']\rangle P_2$$

By induction hypothesis, this implies that one of three cases holds:

(1) $H_1 > (\nu\vec{p})\langle n[H']\rangle P_2$ and $q[Q'_1] = n[H'\{P\}]$. Hence, $q = n$ and $Q'_1 = H'\{P\}$. Since $m \in \mathit{fn}(Q'_1)$ but $m \notin \mathit{fn}(P)$, it follows that $m \in \mathit{fn}(H')$. Note also that $m \notin \mathit{fn}(P_2)$ and that $m \neq n$. So we get:

$$\begin{array}{l} H = (\nu m)H_1 > \overline{(\nu m)}(\nu\vec{p})\langle n[H']\rangle P_2 = (\nu\vec{p})\langle n[(\nu m)H']\rangle P_2 \\ P_1 = q[(\nu m)Q'_1] = n[(\nu m)H'\{P\}] \end{array}$$

This establishes case (1) of the lemma.

(2) $H_1 > (\nu\vec{p})\langle q[Q'_1]\rangle H'$ and $P_2 = H'\{P\}$. From $m \notin \mathit{fn}(Q_2)$ and $Q_2 = P_2 = H'\{P\}$ it follows that $m \notin \mathit{fn}(H')$. So we get:

$$\begin{array}{l} H > \overline{(\nu m)}(\nu\vec{p})\langle q[Q'_1]\rangle H' = (\nu\vec{p})\langle q[(\nu m)Q'_1]\rangle H' = (\nu\vec{p})\langle P_1\rangle H' \\ P_2 = H'\{P\} \end{array}$$

This establishes case (2) of the lemma.

(3) $P > (\nu\vec{p})\langle q[Q'_1]\rangle P'$, $H_1 \equiv - \mid R$, $P_2 \equiv P' \mid R$, and $\{\vec{p}\} \cap \mathit{fn}(R) = \varnothing$. From $P > (\nu\vec{p})\langle q[Q'_1]\rangle P'$ it follows that $\mathit{fn}((\nu\vec{p})\langle q[Q'_1]\rangle P') \subseteq \mathit{fn}(P)$. But we know that $m \in \mathit{fn}(Q'_1)$, $m \notin \{\vec{p}\}$, and $m \notin \mathit{fn}(P)$. Therefore, this case cannot arise.

- Here $m \in \mathit{fn}(Q_1)$, and either (a) $m \in \mathit{fn}(Q_2)$, or (b) Q_1 is not an ambient, or (c) Q_1 is an ambient named m, so that:

$$\begin{array}{rcl} \overline{(\nu m)}(\nu\vec{q})\langle Q_1\rangle Q_2 & = & (\nu m, \vec{q})\langle Q_1\rangle Q_2 \\ & = & (\nu\vec{p})\langle P_1\rangle P_2 \end{array}$$

Therefore, $\vec{p} = m, \vec{q}$, $P_1 = Q_1$, and $P_2 = Q_2$. We have that:

$$H_1\{P\} = Q > (\nu\vec{q})\langle Q_1\rangle Q_2 = (\nu\vec{q})\langle P_1\rangle P_2$$

By induction hypothesis, this implies that one of three cases holds:

(1) $H_1 > (\nu\vec{q})\langle n[H']\rangle P_2$ and $P_1 = n[H'\{P\}]$. We have that:

$$H = (\nu m)H_1 > \overline{(\nu m)}(\nu\vec{q})\langle n[H']\rangle P_2$$

Note that $Q_1 = P_1 = n[H'\{P\}]$. Now, in case (a), $m \in \mathit{fn}(P_2)$ and $m \in \mathit{fn}(n[H'])$ (since $m \notin \mathit{fn}(P)$ but $m \in \mathit{fn}(n[H'\{P\}])$). Case (b) cannot arise, since Q_1 is the ambient $n[H'\{P\}]$. In case (c), it must be that $m = n$. Therefore, in all applicable cases:

$$\overline{(\nu m)}(\nu\vec{q})\langle n[H']\rangle P_2 = (\nu m, \vec{q})\langle n[H']\rangle P_2 = (\nu\vec{p})\langle n[H']\rangle P_2$$

Moreover, $P_1 = n[H'\{P\}]$, which establishes case (1) of the lemma.

(2) $H_1 > (\nu\vec{q})\langle P_1\rangle H'$ and $P_2 = H'\{P\}$. In this case, we have that $m \in fn(P_1)$, and either (a) $m \in fn(H')$ (since $m \in fn(H'\{P\}$ but $m \notin fn(P)$), (b) P_1 is not an ambient, or (c) P_1 is an ambient named m. Hence we have:

$$H = (\nu m)H_1 > \overline{(\nu m)}(\nu\vec{q})\langle P_1\rangle H' = (\nu m, \vec{q})\langle P_1\rangle H'$$

Moreover, $P_2 = H'\{P\}$, which establishes case (2) of the lemma.

(3) $P > (\nu\vec{q})\langle P_1\rangle P'$, $H_1 \equiv - \mid R$, $P_2 \equiv P' \mid R$, and $\{\vec{q}\} \cap fn(R) = \varnothing$. This case cannot arise since $m \notin fn(P)$ and $m \notin \{\vec{q}\}$, so $m \notin fn(P_1)$, and yet we have that $m \in fn(Q_1)$ and $P_1 = Q_1$.

- Here $m \notin fn(Q_1)$, so that:

$$\begin{array}{rcl}\overline{(\nu m)}(\nu\vec{q})\langle Q_1\rangle Q_2 & = & (\nu\vec{q})\langle Q_1\rangle(\nu m)Q_2 \\ & = & (\nu\vec{p})\langle P_1\rangle P_2\end{array}$$

Therefore $\vec{p} = \vec{q}$, $P_1 = Q_1$, and $P_2 = (\nu m)Q_2$. We have that $H_1\{P\} = Q > (\nu\vec{p})\langle P_1\rangle Q_2$. By induction hypothesis, this implies that one of three cases hold:

(1) $H_1 > (\nu\vec{p})\langle n[H']\rangle Q_2$ and $P_1 = n[H'\{P\}]$. We have that $m \notin fn(n[H'\{P\}])$, so

$$\begin{array}{rcl}H & > & \overline{(\nu m)}(\nu\vec{p})\langle n[H']\rangle Q_2 \\ & = & (\nu\vec{p})\langle n[H']\rangle(\nu m)Q_2 \\ & = & (\nu\vec{p})\langle n[H']\rangle P_2\end{array}$$

Also, $P_1 = n[H'\{P\}]$, so this establishes case (1) of the lemma.

(2) $H_1 > (\nu\vec{p})\langle P_1\rangle H'$ and $Q_2 = H'\{P\}$. Here, we have $H > \overline{(\nu m)}(\nu\vec{p})\langle P_1\rangle H' = (\nu\vec{p})\langle P_1\rangle(\nu m)H'$, and $P_2 = (\nu m)H'\{P\} = ((\nu m)H')\{P\}$. This establishes case (2) of the lemma.

(3) $P > (\nu\vec{p})\langle P_1\rangle P'$, $H_1 \equiv - \mid R$, $Q_2 \equiv P' \mid R$, and $\{\vec{p}\} \cap fn(R) = \varnothing$. From $m \notin fn(P) \cup \{\vec{p}\}$ and $P > (\nu\vec{p})\langle P_1\rangle P'$ it follows that $m \notin fn(P')$. We have:

$$H = (\nu m)H_1 \equiv (\nu m)(- \mid R) \equiv - \mid (\nu m)R$$

and also:

$$P_2 = (\nu m)Q_2 \equiv (\nu m)(P' \mid R) \equiv P' \mid (\nu m)R$$

Moreover, $\{\vec{p}\} \cap fn(R) = \varnothing$ implies that $\{\vec{p}\} \cap fn((\nu m)R) = \varnothing$. This establishes case (3) of the lemma.

This completes the proof by induction. □

For the purposes of proving Theorem 15, we adopt the following notation.

Interaction between a harness and a process: $H \bullet P \rightsquigarrow R$

Let $H \bullet P \rightsquigarrow R$ if and only if there are H' and $\vec{r}$ with $\{\vec{r}\} \cap fn(P) = \varnothing$, and one of the following holds:

(Inter In) $H \equiv (\nu\vec{r})H'\{m[- \mid R'] \mid n[R'']\}$, $P \xrightarrow{in\, n} P'$,
and $R \equiv (\nu\vec{r})H'\{n[m[P' \mid R'] \mid R'']\}$

(Inter Out) $H \equiv (\nu\vec{r})H'\{n[m[- \mid R'] \mid R'']\}$, $P \xrightarrow{out\, n} P'$,
and $R \equiv (\nu\vec{r})H'\{m[P' \mid R'] \mid n[R'']\}$

(Inter Open) $H \equiv (\nu\vec{r})H'\{- \mid n[R']\}$, $P \xrightarrow{open\, n} P'$,
and $R \equiv (\nu\vec{r})H'\{P' \mid R'\}$

(Inter Input) $H \equiv (\nu\vec{r})H'\{- \mid \langle M\rangle\}$, $P > (\nu\vec{p})\langle(x).P'\rangle P''$,
and $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(P'\{x{\leftarrow}M\} \mid P'')\}$, with $\{\vec{p}\} \cap fn(M) = \varnothing$

(Inter Output) $H \equiv (\nu\vec{r})H'\{- \mid (x).R'\}$, $P > (\nu\vec{p})\langle\langle M\rangle\rangle P'$,
and $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(P' \mid R'\{x{\leftarrow}M\})\}$, with $\{\vec{p}\} \cap fn(R') = \varnothing$

(Inter Amb) $P > (\nu\vec{p})\langle n[Q]\rangle P'$ and one of the following holds:

(1) $Q \xrightarrow{in\, m} Q'$, $H \equiv (\nu\vec{r})H'\{- \mid m[R']\}$, $\{\vec{p}\} \cap fn(m[R']) = \varnothing$,
and $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(P' \mid m[n[Q'] \mid R'])\}$

(2) $Q \xrightarrow{out\, m} Q'$, $H \equiv (\nu\vec{r})H'\{m[- \mid R']\}$, $m \notin \{\vec{p}\}$,
and $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(n[Q'] \mid m[P' \mid R'])\}$

(3) $H \equiv (\nu\vec{r})H'\{m[R' \mid in\, n.R''] \mid -\}$, $\{\vec{p}\} \cap fn(m[R' \mid in\, n.R'']) = \varnothing$,
and $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(n[Q \mid m[R' \mid R'']] \mid P')\}$

(4) $H \equiv (\nu\vec{r})H'\{- \mid open\, n.R'\}$, $n \notin \{\vec{p}\}$,
and $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(Q \mid P') \mid R'\}$

The following lemmas about the $H \bullet P \rightsquigarrow R$ notation may easily be checked.

Lemma 38 *If $H \bullet P \rightsquigarrow R$ and $R \equiv R'$ then $H \bullet P \rightsquigarrow R'$.*

Lemma 39 *If $H \bullet P \rightsquigarrow R$ then $H'\{H\} \bullet P \rightsquigarrow H'\{R\}$.*

Lemma 40 *If $H \bullet P \rightsquigarrow R$ and $n \notin fn(P)$ then $(\nu n)H \bullet P \rightsquigarrow (\nu n)R$.*

The following lemma is a simple specializations of Lemma 13:

Lemma 41 *If $H\{P\} > (\nu\vec{p})\langle n[P_1]\rangle P_2$ then either:*

(1) *$H \equiv (\nu\vec{p})(n[H'] \mid P_2)$ and $P_1 = H'\{P\}$, or*

(2) *$H \equiv (\nu\vec{p})(n[P_1] \mid H')$ and $P_2 = H'\{P\}$, or*

(3) *$P > (\nu\vec{p})\langle n[P_1]\rangle P'$, $H \equiv - \mid R$, $P_2 \equiv P' \mid R$, and $\{\vec{p}\} \cap fn(R) = \varnothing$.*

The next two lemmas follow from the definition of the M-transitions in terms of hardening.

Lemma 42 *If $H\{P\} \xrightarrow{M} R$ for $M \in \{in\, n, out\, n, open\, n\}$ then either:*

(1) $H \equiv (\nu\vec{r})(M.R' \mid H')$, $R \equiv (\nu\vec{r})(R' \mid H'\{P\})$, $\{\vec{r}\} \cap (\{n\} \cup fn(P)) = \varnothing$, *or*

(2) $H \equiv - \mid R'$, $P \xrightarrow{M} P'$, *and* $R \equiv P' \mid R'$.

Lemma 43 *If $P \mid Q \xrightarrow{M} R$ then either:*

(1) $P \xrightarrow{M} P'$ *and* $R \equiv P' \mid Q$, *or*

(2) $Q \xrightarrow{M} Q'$ *and* $R \equiv P \mid Q'$.

The following proposition is the main fact we need to prove in order to establish Theorem 15.

Proposition 44 *If $H\{P\} \xrightarrow{\tau} R$ then one of the following holds:*

(1) *there is a reduction $P \rightarrow P'$ with $R \equiv H\{P'\}$, or*

(2) *there is a reduction $H \rightarrow H'$ with $R \equiv H'\{P\}$, or*

(3) $H \bullet P \rightsquigarrow R$.

Proof By induction on the derivation of $H\{P\} \xrightarrow{\tau} R$.

(Trans Open) Here, $H\{P\} > (\nu\vec{q})\langle n[Q_1]\rangle Q_2$, and $Q_2 \xrightarrow{open\, n} Q_2'$, and $R = (\nu\vec{q})(Q_1 \mid Q_2')$. We may assume that $\{\vec{q}\} \cap fn(P) = \varnothing$. By Lemma 41, $H\{P\} > (\nu\vec{q})\langle n[Q_1]\rangle Q_2$ implies there are three cases to consider:

(1) $H \equiv (\nu\vec{q})(n[H'] \mid Q_2)$ and $Q_1 = H'\{P\}$. Let $H'' = (\nu\vec{q})(H' \mid Q_2')$. In this case, we can see, for all Q, that $H\{Q\} \rightarrow H''\{Q\}$, which is to say that $H \rightarrow H''$. Moreover, $R \equiv (\nu\vec{q})(H'\{P\} \mid Q_2') \equiv H''\{P\}$. Hence, case (2) pertains.

(2) $H \equiv (\nu\vec{q})(n[Q_1] \mid H_1)$ and $Q_2 = H_1\{P\}$. By Lemma 42, the transition $H_1\{P\} \xrightarrow{open\, n} Q_2'$ implies either:

(a) $H_1 \equiv (\nu\vec{r})(open\, n.R' \mid H_2)$, $Q_2' \equiv (\nu\vec{r})(R' \mid H_2\{P\})$ and $\{\vec{r}\} \cap (\{n\} \cup fn(P)) = \varnothing$. Let $H' = (\nu\vec{q})(Q_1 \mid (\nu\vec{r})(R' \mid H_2))$. We have that $H\{Q\} \rightarrow H'\{Q\}$ for all Q, that is, $H \rightarrow H'$. Moreover, $R \equiv (\nu\vec{q})(Q_1 \mid (\nu\vec{r})(R' \mid H_2\{P\})) \equiv H'\{P\}$. Hence, case (2) pertains.

(b) $H_1 \equiv - \mid R'$, $P \xrightarrow{open\, n} P'$, and $Q_2' \equiv P' \mid R'$. From $H \equiv (\nu\vec{q})(R' \mid - \mid n[Q_1])$, $P \xrightarrow{open\, n} P'$, and $R \equiv (\nu\vec{q})(Q_1 \mid P' \mid R') \equiv (\nu\vec{q})(R' \mid P' \mid Q_1)$ we may derive $H \bullet P \rightsquigarrow R$ using (Inter Open). Hence, case (3) pertains.

(3) $P > (\nu\vec{q})\langle n[Q_1]\rangle P'$, $H \equiv - \mid R'$, $Q_2 \equiv P' \mid R'$, and $\{\vec{q}\} \cap \mathit{fn}(R') = \varnothing$. From $P > (\nu\vec{q})\langle n[Q_1]\rangle P'$ we get $P \equiv (\nu\vec{q})(n[Q_1] \mid P')$. By Lemma 35, $Q_2 \equiv P' \mid R'$ and $Q_2 \xrightarrow{\mathit{open}\,n} Q_2'$ imply there is Q_2'' such that $P' \mid R' \xrightarrow{\mathit{open}\,n} Q_2''$ and $Q_2'' \equiv Q_2'$. By Lemma 43 there are two cases to consider:

(a) $P' \xrightarrow{\mathit{open}\,n} P''$ and $Q_2'' \equiv P'' \mid R'$. We have $P \rightarrow (\nu\vec{q})(Q_1 \mid P'')$, $H \equiv - \mid R'$ and $R \equiv (\nu\vec{q})(Q_1 \mid Q_2') \equiv (\nu\vec{q})(Q_1 \mid P'' \mid R') \equiv (\nu\vec{q})(Q_1 \mid P'') \mid R'$. Hence, case (1) pertains.

(b) $R' \xrightarrow{\mathit{open}\,n} R''$ and $Q_2'' \equiv P' \mid R''$. From $R' \xrightarrow{\mathit{open}\,n} R''$ it follows that $R' \equiv (\nu\vec{r})(R_1 \mid \mathit{open}\,n.R_2)$ with $R'' \equiv (\nu\vec{r})(R_1 \mid R_2)$ and $n \notin \{\vec{r}\}$. We have:

$$\begin{aligned}
H &\equiv (\nu\vec{r})(R_1 \mid - \mid \mathit{open}\,n.R_2) \\
R &\equiv (\nu\vec{q})(Q_1 \mid Q_2') \\
&\equiv (\nu\vec{q})(Q_1 \mid P' \mid R'') \\
&\equiv (\nu\vec{q})(Q_1 \mid P' \mid (\nu\vec{r})(R_1 \mid R_2)) \\
&\equiv (\nu\vec{r})(R_1 \mid (\nu\vec{q})(Q_1 \mid P') \mid R_2)
\end{aligned}$$

since we may assume that $\{\vec{q}\} \cap \mathit{fn}(R_1 \mid R_2) = \varnothing$ and $\{\vec{r}\} \cap \mathit{fn}(Q_1 \mid P') = \varnothing$ and $\{\vec{q}\} \cap \{\vec{r}\} = \varnothing$. From $\{\vec{q}\} \cap \mathit{fn}(R') = \varnothing$ and $R' \xrightarrow{\mathit{open}\,n} R''$ it follows that $n \notin \{\vec{q}\}$. From $P > (\nu\vec{q})\langle n[Q_1]\rangle P'$, $n \notin \{\vec{q}\}$, and the two displayed equations, we may derive $H \bullet P \rightsquigarrow R$ using clause (4) of (Inter Amb). Hence, case (3) pertains.

(Trans Amb) Here, $H\{P\} > (\nu\vec{q})\langle n[Q_1]\rangle Q_2$, $Q_1 \xrightarrow{\tau} Q_1'$ and $R = (\nu\vec{q})(n[Q_1'] \mid Q_2)$. From $H\{P\} > (\nu\vec{q})\langle n[Q_1]\rangle Q_2$ it follows that $\{\vec{q}\} \cap \mathit{fn}(P) = \varnothing$, since $\mathit{fn}(P) \subseteq \mathit{fn}(H\{P\})$. By Lemma 13, $H\{P\} > (\nu\vec{q})\langle n[Q_1]\rangle Q_2$ implies there are three cases to consider:

(1) $H > (\nu\vec{q})\langle n[H']\rangle Q_2$ and $Q_1 = H'\{P\}$. By induction hypothesis, $Q_1 = H'\{P\} \xrightarrow{\tau} Q_1'$ implies one of the following:

(a) Here $P \rightarrow P'$ with $Q_1' \equiv H'\{P'\}$. We have $R \equiv (\nu\vec{q})(n[H'\{P'\}] \mid Q_2)$, and $H \equiv (\nu\vec{q})(n[H'] \mid Q_2)$ so case (1) pertains.

(b) Here $H' \rightarrow H''$ with $Q_1' \equiv H''\{P\}$. From $H > (\nu\vec{q})\langle n[H']\rangle Q_2$ and $H' \rightarrow H''$ we can derive $H \rightarrow (\nu\vec{q})(n[H''] \mid Q_2)$. We have $R \equiv (\nu\vec{q})(n[H''\{P\}] \mid Q_2)$, so case (2) pertains.

(c) Here $H' \bullet P \rightsquigarrow Q_1'$. From $H > (\nu\vec{q})\langle n[H']\rangle Q_2$ we get that $H \equiv (\nu\vec{q})(n[H'] \mid Q_2)$. Also, $R \equiv (\nu\vec{q})(n[Q_1'] \mid Q_2)$. By Lemma 39, $H' \bullet P \rightsquigarrow Q_1'$ implies that $n[H'] \mid Q_2 \bullet P \rightsquigarrow n[Q_1'] \mid Q_2$. By Lemma 40, $\{\vec{q}\} \cap \mathit{fn}(P) = \varnothing$ implies that $(\nu\vec{q})(n[H'] \mid Q_2) \bullet P \rightsquigarrow (\nu\vec{q})(n[Q_1'] \mid Q_2)$. By Lemma 38, $H \bullet P \rightsquigarrow R$. Hence case (3) pertains.

(2) $H > (\nu\vec{q})\langle n[Q_1]\rangle H_1$ and $Q_2 = H_1\{P\}$. Let $H' = (\nu\vec{q})(n[Q_1'] \mid H_1)$. Since $H \equiv (\nu\vec{q})(n[Q_1] \mid H_1)$ and $Q_1 \xrightarrow{\tau} Q_1'$, we get that $H \rightarrow$

H'. Moreover, $R \equiv (\nu\vec{q})(n[Q_1'] \mid H_1\{P\}) \equiv H'\{P\}$. Hence case (2) pertains.

(3) $P > (\nu\vec{q})\langle n[Q_1]\rangle P'$, $H \equiv - \mid R'$, $Q_2 \equiv P' \mid R'$, and $\{\vec{q}\} \cap fn(R') = \varnothing$. Let $P' = (\nu\vec{q})(n[Q_1'] \mid P')$. From $Q_1 \xrightarrow{\tau} Q_1'$ and $P \equiv (\nu\vec{p})(n[Q_1] \mid P')$, we get that $P \to P'$. Moreover, $R \equiv (\nu\vec{q})(n[Q_1'] \mid P' \mid R') \equiv H\{P'\}$. Hence case (1) pertains.

The cases for the rules (Trans In), (Trans Out), and (Trans I/O) are proved by arguments similar to that for (Trans Open). Since the rule (Trans Cap) cannot derive a τ-transition, this completes the analysis of all the rules that may derive $H\{P\} \xrightarrow{\tau} R$. □

We now prove Theorem 15, which we restate in terms of the interaction predicate, $H \bullet P \leadsto R$.

Proof of Theorem 15 *$H\{P\} \to R$ if and only if:*

(Act Proc) *$P \to P'$ with $R \equiv H\{P'\}$, or*

(Act Har) *$H \to H'$ with $R \equiv H'\{P\}$, or*

(Act Inter) *$H \bullet P \leadsto R$.*

Proof The right-to-left direction is a routine calculation. For the left-to-right direction, suppose that $H\{P\} \to R$. By Theorem 9, there is Q with $H\{P\} \xrightarrow{\tau} Q$ and $Q \equiv R$. By Proposition 44, there are three cases to consider:

(1) There is a reduction $P \to P'$ with $Q \equiv H\{P'\}$. From $Q \equiv R$ we get $R \equiv H\{P'\}$, so (Act Proc) applies.

(2) There is a reduction $H \to H'$ with $Q \equiv H'\{P\}$. From $Q \equiv R$ we get $R \equiv H\{P'\}$, so (Act Har) applies.

(3) We have $H \bullet P \leadsto Q$. By Lemma 38, $Q \equiv R$ implies that $H \bullet P \leadsto R$. Therefore, (Act Inter) applies. □

A.5 Proofs About Replication

In this section, we prove a series of lemmas about replicated processes. These lemmas are needed in the next section, in the proof of Proposition 61, that the equivalence implicit in the context lemma is a congruence with respect to replication.

We use the notation P^k as an abbreviation for k copies of P running in parallel: we inductively define $P^0 \triangleq \mathbf{0}$, and $P^{k+1} \triangleq P \mid P^k$.

Lemma 45 *If $!P > (\nu\vec{p})\langle Q\rangle R$ then there is P' such that $P > (\nu\vec{p})\langle Q\rangle P'$ with $R = P' \mid !P$ and $\{\vec{p}\} \cap fn(P) = \varnothing$.*

Proof The judgment $!P > (\nu\vec{p})\langle Q\rangle R$ can only be derived using the rule (Harden Repl), from a judgment $!P > (\nu\vec{p})\langle Q\rangle P'$ such that $R = P' \mid !P$. By Lemma 22, $!P > (\nu\vec{p})\langle Q\rangle P'$ implies that $fn(!P) = fn((\nu\vec{p})\langle Q\rangle P')$, and therefore that $\{\vec{p}\} \cap fn(P) = \varnothing$. □

Lemma 46 *If* $!P \xrightarrow{M} Q$ *then there is* R *such that* $P \xrightarrow{M} R$ *and* $Q \equiv R \mid !P$.

Proof The judgment $!P \xrightarrow{M} Q$ can only be derived using (Trans Cap) from a judgment $!P > (\nu\vec{p})\langle M.P'\rangle P''$ with $fn(M) \cap \{\vec{p}\} = \varnothing$ and $Q = (\nu\vec{p})(P' \mid P'')$. By Lemma 45, there is P''' with $P > (\nu\vec{p})\langle M.P'\rangle P'''$, $P'' = P''' \mid !P$, and $\{\vec{p}\} \cap fn(P) = \varnothing$. Let $R = (\nu\vec{p})(P' \mid P''')$. By (Trans Cap), we have $P \xrightarrow{M} R$. Moreover, $Q = (\nu\vec{p})(P' \mid P''' \mid !P) \equiv R \mid !P$. □

Lemma 47 *If* $!P \xrightarrow{\tau} Q$ *then there is* R *with* $P \mid P \xrightarrow{\tau} R$ *and* $Q \equiv R \mid !P$.

Proof By a case analysis of the derivation of $!P \xrightarrow{\tau} Q$.

(Trans Amb) Here, $!P \xrightarrow{\tau} (\nu\vec{p})(n[Q'] \mid P')$ derives from $!P > (\nu\vec{p})\langle n[Q]\rangle P'$ and $Q \xrightarrow{\tau} Q'$. By Lemma 45, $!P > (\nu\vec{p})\langle n[Q]\rangle P'$ implies there is R' such that $P > (\nu\vec{p})\langle n[Q]\rangle R'$, $P' = R' \mid !P$, and $fn(P) \cap \{\vec{p}\} = \varnothing$. By (Harden Par 1), $P > (\nu\vec{p})\langle n[Q]\rangle R'$ and $\{\vec{p}\} \cap fn(P) = \varnothing$ imply that $P \mid P > (\nu\vec{p})\langle n[Q]\rangle(R' \mid P)$. By (Trans Amb), this and $Q \xrightarrow{\tau} Q'$ imply that $P \mid P \xrightarrow{\tau} R$, where $R = (\nu\vec{p})(n[Q'] \mid R' \mid P)$. Finally, we may calculate: $(\nu\vec{p})(n[Q'] \mid P') = (\nu\vec{p})(n[Q'] \mid R' \mid !P) \equiv (\nu\vec{p})(n[Q'] \mid R' \mid P \mid !P) \equiv R \mid !P$.

(Trans In) Here, $!P \xrightarrow{\tau} (\nu\vec{p},\vec{r})(m[n[Q'] \mid R_1] \mid R_2)$ derives from the judgments $!P > (\nu\vec{p})\langle n[Q]\rangle R$, $Q \xrightarrow{in\ m} Q'$, and $R > (\nu\vec{r})\langle m[R_1]\rangle R_2$, with $\{\vec{r}\} \cap fn(n[Q]) = \varnothing$ and $\{\vec{r}\} \cap \{\vec{p}\} = \varnothing$. By Lemma 45, $!P > (\nu\vec{p})\langle n[Q]\rangle R$ implies there is R' such that $P > (\nu\vec{p})\langle n[Q]\rangle R'$ and $R \equiv R' \mid !P$ with $\{\vec{p}\} \cap fn(P) = \varnothing$.

By Lemma 31 and (Struct Symm), $R > (\nu\vec{r})\langle m[R_1]\rangle R_2$ and $R \equiv R' \mid !P$ imply there are R_1' and R_2' such that $R' \mid !P > (\nu\vec{r})\langle m[R_1']\rangle R_2'$, $R_1 \equiv R_1'$, and $R_2 \equiv R_2'$. Only two rules may derive the judgment $R' \mid !P > (\nu\vec{r})\langle m[R_1']\rangle R_2'$:

(Harden Par 1) In this case, $R' > (\nu\vec{r})\langle m[R_1']\rangle R''$ with $R_2' = R'' \mid !P$ and $\{\vec{r}\} \cap fn(!P) = \varnothing$. By (Harden Par 1), $P > (\nu\vec{p})\langle n[Q]\rangle R'$ and $\{\vec{p}\} \cap fn(P) = \varnothing$ imply that $P \mid P > (\nu\vec{p})\langle n[Q]\rangle(R' \mid P)$. By (Harden Par 1), $R' > (\nu\vec{r})\langle m[R_1']\rangle R''$ and $\{\vec{r}\} \cap fn(P) = \varnothing$ imply that $R' \mid P > (\nu\vec{r})\langle m[R_1']\rangle(R'' \mid P)$. By (Trans In), $P \mid P > (\nu\vec{p})\langle n[Q]\rangle(R' \mid P)$, $Q \xrightarrow{in\ m} Q'$, and $R' \mid P > (\nu\vec{r})\langle m[R_1']\rangle(R'' \mid P)$ imply that $P \mid P \xrightarrow{\tau} (\nu\vec{p},\vec{r})(m[n[Q'] \mid R_1'] \mid R'' \mid P)$. We know that $fn(P) \cap \{\vec{p},\vec{r}\} = \varnothing$, and hence we may calculate:

$$\begin{array}{rcl}(\nu\vec{p},\vec{r})(m[n[Q'] \mid R_1] \mid R_2) & \equiv & (\nu\vec{p},\vec{r})(m[n[Q'] \mid R_1'] \mid R_2') \\ & = & (\nu\vec{p},\vec{r})(m[n[Q'] \mid R_1'] \mid R'' \mid !P) \\ & \equiv & (\nu\vec{p},\vec{r})(m[n[Q'] \mid R_1'] \mid R'' \mid P) \mid !P\end{array}$$

(Harden Par 2) In this case, $!P > (\nu\vec{r})\langle m[R_1']\rangle R''$ with $R_2' = R' \mid R''$ and $\{\vec{r}\} \cap \mathit{fn}(!P) = \varnothing$. By Lemma 45, $!P > (\nu\vec{r})\langle m[R_1']\rangle R''$ implies there is R''' such that $P > (\nu\vec{r})\langle m[R_1']\rangle R'''$ with $R'' = R''' \mid !P$ and $\{\vec{r}\} \cap \mathit{fn}(P) = \varnothing$. By (Harden Par 1), $P > (\nu\vec{p})\langle n[Q]\rangle R'$ and $\{\vec{p}\} \cap \mathit{fn}(P) = \varnothing$ imply that $P \mid P > (\nu\vec{p})\langle n[Q]\rangle (R' \mid P)$. By Lemma 20 and Lemma 22, $R > (\nu\vec{r})\langle m[R_1]\rangle R_2$ and $R \equiv R' \mid !P$ imply that $\mathit{fn}(R') \cap \{\vec{r}\} = \varnothing$. By (Harden Par 2), this and $P > (\nu\vec{r})\langle m[R_1']\rangle R'''$ imply that $R' \mid P > (\nu\vec{r})\langle m[R_1']\rangle (R' \mid R''')$. By (Trans In), $P \mid P > (\nu\vec{p})\langle n[Q]\rangle (R' \mid P)$, $Q \xrightarrow{in\ m} Q'$, and $R' \mid P > (\nu\vec{r})\langle m[R_1']\rangle (R' \mid R''')$ imply $P \mid P \xrightarrow{\tau} (\nu\vec{p},\vec{r})(m[n[Q'] \mid R_1'] \mid R' \mid R''')$. We know that $\mathit{fn}(P) \cap \{\vec{p},\vec{r}\} = \varnothing$, and hence we may calculate:

$$\begin{array}{cl}
\multicolumn{2}{l}{(\nu\vec{p},\vec{r})(m[n[Q'] \mid R_1] \mid R_2)} \\
\equiv & (\nu\vec{p},\vec{r})(m[n[Q'] \mid R_1'] \mid R' \mid R'') \\
= & (\nu\vec{p},\vec{r})(m[n[Q'] \mid R_1'] \mid R' \mid (R''' \mid !P)) \\
\equiv & (\nu\vec{p},\vec{r})(m[n[Q'] \mid R_1'] \mid R' \mid R''') \mid !P
\end{array}$$

The other cases—(Trans Out), (Trans Open), and (Trans I/O)—follow by similar arguments. □

Lemma 48 *If $H\{!P\} \to R$ then there is H' such that $R \equiv H'\{!P\}$ and for all k, $H\{P^{k+2}\} \to H'\{P^k\}$.*

Proof By Theorem 15, $H\{!P\} \to R$ implies that one of three cases holds:

(Act Proc) Here, $!P \to P'$ with $R \equiv H\{P'\}$. By Lemma 47 and Theorem 9, $!P \to P'$ implies there is Q with $P \mid P \to Q$ and $P' \equiv Q \mid !P$. Let $H' = H\{Q \mid -\}$. We have $R \equiv H\{Q \mid !P\} = H'\{!P\}$. For any k, we have $P \mid P \mid P^k \to Q \mid P^k$. This implies that $H\{P^{k+2}\} \to H\{Q \mid P^k\}$, which itself implies that $H\{P^{k+2}\} \to H'\{P^k\}$.

(Act Har) Here, $H \to H''$ with $R \equiv H''\{!P\}$. Let $H' = H''\{P \mid P \mid -\}$. Then $R \equiv H''\{P \mid P \mid !P\} = H'\{!P\}$, and, for all k, $H\{P^{k+2}\} \to H''\{P^{k+2}\} \equiv H'\{P^k\}$.

(Act Inter) Here, there are H_0 and $\vec{r}$ with $\{\vec{r}\} \cap \mathit{fn}(P) = \varnothing$, and one of the following holds:

(Inter In) In this case, $H \equiv (\nu\vec{r})H_0\{m[- \mid R'] \mid n[R'']\}$, $!P \xrightarrow{in\ n} P'$, $R \equiv (\nu\vec{r})H_0\{n[m[P' \mid R'] \mid R'']\}$. By Lemma 46, there is Q such that $P \xrightarrow{in\ n} Q$ and $P' \equiv Q \mid !P$. Let $H' = (\nu\vec{r})H_0\{n[m[- \mid P \mid Q \mid R'] \mid R'']\}$, and we have, for all k:

$$\begin{array}{rcl}
R & \equiv & (\nu\vec{r})H_0\{n[m[Q \mid !P \mid R'] \mid R'']\} \\
 & \equiv & (\nu\vec{r})H_0\{n[m[!P \mid P \mid Q \mid R'] \mid R'']\} \\
 & = & H'\{!P\}
\end{array}$$

$$\begin{aligned} H\{P^{k+2}\} &\equiv (\nu\vec{r})H_0\{m[P^k \mid P \mid P \mid R'] \mid n[R'']\} \\ &\rightarrow (\nu\vec{r})H_0\{n[m[P^k \mid P \mid Q \mid R'] \mid R'']\} \\ &\equiv H'\{P^k\} \end{aligned}$$

(Inter Out) In this case, $H \equiv (\nu\vec{r})H_0\{n[m[- \mid R'] \mid R'']\}$, $!P \xrightarrow{out\,n} P'$, and $R \equiv (\nu\vec{r})H_0\{m[P' \mid R'] \mid n[R'']\}$. By Lemma 46, there is Q such that $P \xrightarrow{out\,n} Q$ and $P' \equiv Q \mid !P$. Let $H' = (\nu\vec{r})H_0\{m[- \mid P \mid Q \mid R'] \mid n[R'']\}$, and we have, for all k:

$$\begin{aligned} R &\equiv (\nu\vec{r})H_0\{m[!P \mid Q \mid R'] \mid n[R'']\} \\ &\equiv (\nu\vec{r})H_0\{m[!P \mid P \mid Q \mid R'] \mid n[R'']\} \\ &= H'\{!P\} \\ H\{P^{k+2}\} &\equiv (\nu\vec{r})H_0\{n[m[P^k \mid P \mid P \mid R'] \mid R'']\} \\ &\rightarrow (\nu\vec{r})H_0\{m[P^k \mid P \mid Q \mid R'] \mid n[R'']\} \\ &\equiv H'\{P^k\} \end{aligned}$$

(Inter Open) In this case, $H \equiv (\nu\vec{r})H_0\{- \mid n[R']\}$, $!P \xrightarrow{open\,n} P'$, and $R \equiv (\nu\vec{r})H_0\{P' \mid R'\}$. By Lemma 46, there is Q such that $P \xrightarrow{open\,n} Q$ and $P' \equiv Q \mid !P$. Let $H' = (\nu\vec{r})H_0\{- \mid P \mid Q \mid R'\}$, and we have, for all k:

$$\begin{aligned} R &\equiv (\nu\vec{r})H_0\{Q \mid !P \mid R'\} \\ &\equiv (\nu\vec{r})H_0\{!P \mid P \mid Q \mid R'\} \\ &= H'\{!P\} \\ H\{P^{k+2}\} &\equiv (\nu\vec{r})H_0\{P^k \mid P \mid P \mid n[R']\} \\ &\rightarrow (\nu\vec{r})H_0\{P^k \mid P \mid Q \mid R'\} \\ &\equiv H'\{P^k\} \end{aligned}$$

(Inter Input) In this case, $H \equiv (\nu\vec{r})H_0\{- \mid \langle M\rangle\}$, $!P > (\nu\vec{p})\langle(x).P'\rangle P''$, and $R \equiv (\nu\vec{r})H_0\{(\nu\vec{p})(P'\{x{\leftarrow}M\} \mid P'')\}$, with $\{\vec{p}\} \cap fn(M) = \varnothing$. By Lemma 45, there is Q such that $P > (\nu\vec{p})\langle(x).P'\rangle Q$ with $P'' = Q \mid !P$ and $\{\vec{p}\} \cap fn(P) = \varnothing$. Let $H' = (\nu\vec{r})H_0\{- \mid P \mid (\nu\vec{p})(P'\{x{\leftarrow}M\} \mid Q)\}$, and we have, for all k:

$$\begin{aligned} R &\equiv (\nu\vec{r})H_0\{(\nu\vec{p})(P'\{x{\leftarrow}M\} \mid Q \mid !P)\} \\ &\equiv (\nu\vec{r})H_0\{!P \mid P \mid (\nu\vec{p})(P'\{x{\leftarrow}M\} \mid Q)\} \\ &= H'\{!P\} \\ H\{P^{k+2}\} &\equiv (\nu\vec{r})H_0\{P^k \mid P \mid P \mid \langle M\rangle\} \\ &\rightarrow (\nu\vec{r})H_0\{P^k \mid P \mid (\nu\vec{p})(P'\{x{\leftarrow}M\} \mid Q)\} \\ &\equiv H'\{P^k\} \end{aligned}$$

(Inter Output) Here, $H \equiv (\nu\vec{r})H_0\{- \mid (x).R'\}$, $!P > (\nu\vec{p})\langle\langle M\rangle\rangle P'$, and $R \equiv (\nu\vec{r})H_0\{(\nu\vec{p})(P' \mid R'\{x{\leftarrow}M\})\}$, with $\{\vec{p}\} \cap fn(R') = \varnothing$.

By Lemma 45, there is Q such that $P > (\nu\vec{p})\langle\langle M\rangle\rangle Q$ with $P' = Q \mid !P$ and $\{\vec{p}\} \cap fn(P) = \varnothing$. Let $H' = (\nu\vec{r})H_0\{- \mid P \mid (\nu\vec{p})(Q \mid R'\{x\leftarrow M\})\}$, and we have, for all k:

$$\begin{array}{rcl}
R & \equiv & (\nu\vec{r})H_0\{(\nu\vec{p})(Q \mid !P \mid R'\{x\leftarrow M\})\} \\
 & \equiv & (\nu\vec{r})H_0\{!P \mid P \mid (\nu\vec{p})(Q \mid R'\{x\leftarrow M\})\} \\
 & = & H'\{!P\} \\
H\{P^{k+2}\} & \equiv & (\nu\vec{r})H_0\{P^k \mid P \mid P \mid (x).R'\} \\
 & \rightarrow & (\nu\vec{r})H_0\{P^k \mid P \mid (\nu\vec{p})(Q \mid R'\{x\leftarrow M\})\} \\
 & \equiv & H'\{P^k\}
\end{array}$$

(Inter Amb) In this case, one of the following four cases holds, and we have $!P > (\nu\vec{p})\langle n[Q]\rangle P'$ and $n \notin \{\vec{p}\}$, which by Lemma 45 implies that there is P'' such that $P > (\nu\vec{p})\langle n[Q]\rangle P''$ with $P' = P'' \mid !P$ and $\{\vec{p}\} \cap fn(P) = \varnothing$.

(1) Here, $Q \xrightarrow{in\ m} Q'$, $H \equiv (\nu\vec{r})H_0\{- \mid m[R']\}$, $\{\vec{p}\} \cap fn(m[R']) = \varnothing$, and $R \equiv (\nu\vec{r})H_0\{(\nu\vec{p})(P' \mid m[n[Q'] \mid R'])\}$. Let $H' = (\nu\vec{r})H_0\{- \mid P \mid (\nu\vec{p})(P'' \mid m[n[Q'] \mid R'])\}$ and we get, for all k:

$$\begin{array}{rcl}
R & \equiv & (\nu\vec{r})H_0\{(\nu\vec{p})(P'' \mid !P \mid m[n[Q'] \mid R'])\} \\
 & \equiv & (\nu\vec{r})H_0\{!P \mid P \mid (\nu\vec{p})(P'' \mid m[n[Q'] \mid R'])\} \\
 & \equiv & H'\{!P\} \\
H\{P^{k+2}\} & = & (\nu\vec{r})H_0\{P^k \mid P \mid P \mid m[R']\} \\
 & \rightarrow & (\nu\vec{r})H_0\{P^k \mid P \mid (\nu\vec{p})(P'' \mid m[n[Q'] \mid R'])\} \\
 & \equiv & H'\{P^k\}
\end{array}$$

(2) In this case, $Q \xrightarrow{out\ m} Q'$, $H \equiv (\nu\vec{r})H_0\{m[- \mid R']\}$, and $R \equiv (\nu\vec{r})H_0\{(\nu\vec{p})(n[Q'] \mid m[P' \mid R'])\}$, with $m \notin \{\vec{p}\}$. Let $H' = (\nu\vec{r})H_0\{(\nu\vec{p})(n[Q'] \mid m[P'' \mid P \mid - \mid R'])\}$ and we get, for all k:

$$\begin{array}{rcl}
R & \equiv & (\nu\vec{r})H_0\{(\nu\vec{p})(n[Q'] \mid m[P'' \mid !P \mid R'])\} \\
 & \equiv & (\nu\vec{r})H_0\{(\nu\vec{p})(n[Q'] \mid m[P'' \mid P \mid !P \mid R'])\} \\
 & = & H'\{!P\} \\
H\{P^{k+2}\} & \equiv & (\nu\vec{r})H_0\{m[P \mid P \mid P^k \mid R']\} \\
 & \rightarrow & (\nu\vec{r})H_0\{(\nu\vec{p})(n[Q'] \mid m[P'' \mid P \mid P^k \mid R'])\} \\
 & \equiv & H'\{P^k\}
\end{array}$$

(3) $H \equiv (\nu\vec{r})H_0\{m[R' \mid in n.R''] \mid -\}$, $\{\vec{p}\} \cap fn(m[R' \mid in n.R'']) = \varnothing$, and $R \equiv (\nu\vec{r})H_0\{(\nu\vec{p})(n[Q \mid m[R' \mid R'']] \mid P')\}$. Let $H' = (\nu\vec{r})H_0\{(\nu\vec{p})(n[Q \mid m[R' \mid R'']] \mid P'') \mid P \mid -\}$ and we get, for all k:

$$\begin{array}{rcl}
R & \equiv & (\nu\vec{r})H_0\{(\nu\vec{p})(n[Q \mid m[R' \mid R'']] \mid P'' \mid !P)\}
\end{array}$$

$$\begin{array}{rl}
\equiv & (\nu\vec{r})H_0\{(\nu\vec{p})(n[Q \mid m[R' \mid R'']] \mid P'') \mid P \mid !P\} \\
= & H'\{!P\} \\
\multicolumn{2}{l}{H\{P^{k+2}\}} \\
\equiv & (\nu\vec{r})H_0\{m[R' \mid \mathit{in}\, n.R''] \mid P \mid P \mid P^k\} \\
\rightarrow & (\nu\vec{r})H_0\{(\nu\vec{p})(n[Q \mid m[R' \mid \mathit{in}\, n.R'']] \mid P'') \mid P \mid P^k\} \\
\equiv & H'\{P^k\}
\end{array}$$

(4) $H \equiv (\nu\vec{r})H_0\{- \mid \mathit{open}\, n.R'\}$, and $R \equiv (\nu\vec{r})H_0\{(\nu\vec{p})(Q \mid P') \mid R'\}$ Let $H' = (\nu\vec{r})H_0\{(\nu\vec{p})(Q \mid P'') \mid R' \mid P \mid -\}$ and we get, for all k:

$$\begin{array}{rcl}
R & \equiv & (\nu\vec{r})H_0\{(\nu\vec{p})(Q \mid P'' \mid !P) \mid R'\} \\
 & \equiv & (\nu\vec{r})H_0\{(\nu\vec{p})(Q \mid P'') \mid R' \mid P \mid !P\} \\
 & = & H'\{!P\} \\
H\{P^{k+2}\} & \equiv & (\nu\vec{r})H_0\{P^k \mid P \mid P \mid \mathit{open}\, n.R'\} \\
 & \rightarrow & (\nu\vec{r})H_0\{P^k \mid P \mid (\nu\vec{p})(Q \mid P'') \mid R'\} \\
 & \equiv & H'\{P^k\}
\end{array}$$

In any case, then, the result holds. □

Lemma 49 *If $H\{!P\} \Downarrow n$ then there is k such that $H\{P^k\} \Downarrow n$.*

Proof By induction on the derivation of $H\{!P\} \Downarrow n$.

(Conv Exh) Here, $H\{!P\} \downarrow n$. By Proposition 14, this implies that either (1) $H\{Q\} \downarrow n$ for all Q, or (2) $!P \downarrow n$, and for all Q, $Q \downarrow n$ implies that $H\{Q\} \downarrow n$. In case (1), let $k = 1$ and we have $H\{P\} \downarrow n$. In case (2), Proposition 7 implies that $!P > (\nu\vec{p})\langle n[P']\rangle P''$ with $n \notin \{\vec{p}\}$, for some names $\vec{p}$ and processes P' and P''. By Lemma 45, it follows that there is P''' such that $P > (\nu\vec{p})\langle n[P']\rangle P'''$ with $P'' = P''' \mid !P$ and $\{\vec{p}\} \cap \mathit{fn}(P) = \varnothing$. Proposition 7 now yields that $P \downarrow n$. Let $k = 1$ and we get that $H\{P\} \downarrow n$.

(Conv Red) Here, $H\{!P\} \rightarrow Q$ and $Q \Downarrow n$. By Lemma 48, $H\{!P\} \rightarrow Q$ implies there is H' such that $Q \equiv H'\{!P\}$ and, for all j, $H\{P^{j+2}\} \rightarrow H'\{P^j\}$. By Lemma 2, there is a derivation of $H'\{!P\} \Downarrow n$ with the same depth of inference as the derivation of $Q \Downarrow n$. By induction hypothesis, there is k such that $H'\{P^k\} \Downarrow n$. Now, we have that $H\{P^{k+2}\} \rightarrow H'\{P^k\}$. By (Conv Red), this and $H'\{P^k\} \Downarrow n$ imply that $H\{P^{k+2}\} \Downarrow n$. □

A.6 Proofs Omitted From Section 4.3

The purpose of this section is to prove our context lemma, Theorem 12. Roughly speaking, the context lemma asserts that the distinctions made by all contexts are the same as the distinctions made by harnesses. To prove the context lemma, it is convenient to introduce the following auxiliary equivalence, defined in terms of harnesses. Recall that a *substitution*, σ, be a list $x_1 \leftarrow M_1, \ldots, x_k \leftarrow M_k$, where the variables $x_1, \ldots, x_k$ are pairwise distinct, and $fv(M_i) = \varnothing$ for each $i \in 1..k$.

The Equivalence Implicit in the Context Lemma: $P \sim Q$

Let $P \sim Q$ if and only if for all substitutions σ with $dom(\sigma) = fv(P) \cup fv(Q)$, and for all closed harnesses H and names n, that $H\{P\sigma\} \Downarrow n \Leftrightarrow H\{Q\sigma\} \Downarrow n$.

Next, we prove a series of lemmas, which taken together imply Proposition 64, that the auxiliary equivalence $P \sim Q$ is a congrence. The context lemma then follows easily.

Proposition 50 *The relation $P \sim Q$ is an equivalence, that is, reflexive, transitive, and symmetric. Moreover, if $P \equiv Q$ then $P \sim Q$.*

Proof That $P \sim Q$ is an equivalence follows easily from its definition. Suppose that $P \equiv Q$. Consider any substitution σ such that $fv(P) \cup fv(Q) = dom(\sigma)$. Structural congruence is preserved by substitutions, so $P\sigma \equiv Q\sigma$. Moreover, structural congruence is a congruence, so $H\{P\sigma\} \equiv H\{Q\sigma\}$. By Lemma 2, it follows that for all n, $H\{P\sigma\} \Downarrow n \Leftrightarrow H\{Q\sigma\} \Downarrow n$. Therefore, $P \sim Q$. □

Proposition 51 *If $P \sim P'$ then $P \mid Q \sim P' \mid Q$.*

Proof Consider any substitution σ with $dom(\sigma) = fv(P \mid Q) \cup fv(P' \mid Q)$, and any closed harness H and any name n. Let $H' = H\{- \mid Q\sigma\}$. Since $fv(Q) \subset dom(\sigma)$, the harness H' is closed. Let σ' be the restriction of σ to the domain $fv(P) \cup fv(P')$. We have that:

$$\begin{aligned} H\{(P \mid Q)\sigma\} &= H'\{P\sigma'\} \\ H\{(P' \mid Q)\sigma\} &= H'\{P'\sigma'\} \end{aligned}$$

Now, suppose $H\{(P \mid Q)\sigma\} \Downarrow n$, that is, $H'\{P\sigma'\} \Downarrow n$. This and $P \sim P'$ imply that $H'\{P'\sigma'\} \Downarrow n$, which is to say, $H\{(P' \mid Q)\sigma\} \Downarrow n$. A symmetric argument establishes that $H\{(P' \mid Q)\sigma\} \Downarrow n$ implies $H\{(P \mid Q)\sigma\} \Downarrow n$. Therefore, $P \mid Q \sim P' \mid Q$. □

Lemma 52 *If $m \neq n$, then $(\nu n)P \Downarrow m \Leftrightarrow P \Downarrow m$.*

Proof An induction on the derivation of $P \Downarrow m$ establishes that $(\nu n)P \Downarrow m$, using (Red Res) and Proposition 6. On the other hand, an induction on the derivation of $(\nu n)P \Downarrow m$ establishes that $P \Downarrow m$, using Theorem 9 and Lemma 36. □

Proposition 53 *If $P \sim P'$ then $(\nu n)P \sim (\nu n)P'$.*

Proof Consider any substitution σ with $dom(\sigma) = fv((\nu n)P) \cup fv((\nu n)P')$, that is, $dom(\sigma) = fv(P) \cup fv(P')$. Consider any closed harness H and any name m. Since the name n is bound, we may assume that $n \notin fn(\sigma(x))$ for all $x \in dom(\sigma)$, that $n \notin fn(H)$ and that $m \neq n$. We have that:

$$\begin{array}{rcl} H\{((\nu n)P)\sigma\} & = & (\nu n)(H\{P\sigma\}) \\ H\{((\nu n)P')\sigma\} & = & (\nu n)(H\{P'\sigma\}) \end{array}$$

By definition of $P \sim P'$, it follows that $H\{P\sigma\} \Downarrow m \Leftrightarrow H\{P'\sigma\} \Downarrow m$. By Lemma 52, it follows that $(\nu n)(H\{P\sigma\}) \Downarrow m \Leftrightarrow (\nu n)(H\{P'\sigma\}) \Downarrow m$, which is to say that $H\{((\nu n)P)\sigma\} \Downarrow m \Leftrightarrow H\{((\nu n)P')\sigma\} \Downarrow m$. It follows that $(\nu n)P \sim (\nu n)P'$. □

Lemma 54 *If M is not a name and $H\{M[P]\} \Downarrow m$ then $H\{\mathbf{0}\} \Downarrow m$.*

Proof By induction on the derivation of $H\{M[P]\} \Downarrow m$, with appeal to the activity lemma, Theorem 15. An ambient $M[P]$, where M is not a name, cannot participate in any transitions. □

Proposition 55 *If $P \sim P'$ then $M[P] \sim M[P']$.*

Proof Consider any substitution σ with $dom(\sigma) = fv(M[P]) \cup fv(M[P'])$, that is, $dom(\sigma) = fv(M) \cup fv(P) \cup fv(P')$. Consider any closed harness H and any name m. Either $M\sigma$ is a name n, or not. If not, we get that $H\{(M[P])\sigma\} \Downarrow m \Leftrightarrow H\{\mathbf{0}\} \Downarrow m \Leftrightarrow H\{(M[P'])\sigma\} \Downarrow m$ from Lemma 18 and Lemma 54. On the other hand, suppose that $M\sigma$ is the name n. Let $H' = H\{n[-]\}$. Given that H is closed, so is H'. We have that:

$$\begin{array}{rcl} H\{(M[P])\sigma\} & = & H'\{P\sigma\} \\ H\{(M[P'])\sigma\} & = & H'\{P'\sigma\} \end{array}$$

Now, suppose $H\{(M[P])\sigma\} \Downarrow m$, that is, $H'\{P\sigma\} \Downarrow m$. This and $P \sim P'$ imply that $H'\{P'\sigma\} \Downarrow m$, which is to say, $H\{(M[P'])\sigma\} \Downarrow m$. A symmetric argument establishes that $H\{(n[P'])\sigma\} \Downarrow m$ implies $H\{(n[P])\sigma\} \Downarrow m$. Therefore, whether or not M is a name, $M[P] \sim M[P']$. □

The relation $M > \epsilon$ in the following lemma is as defined in Appendix A.2.

Lemma 56 *$M.P \to Q$ if and only if $M > \epsilon$ and $P \to Q$.*

Proof The right-to-left direction follows from the fact that $M > \epsilon$ implies that $M.P \equiv P$. For the other direction, $M.P \to Q$ implies, by Theorem 9 that there is R with $M.P \xrightarrow{\tau} R$ and $R \equiv Q$. An inspection of the rules for deriving τ-transitions reveals that the first step in deriving $M.P \xrightarrow{\tau} R$ is a hardening $M.P > C$, where the prime of the concretion C is either an ambient or an output. Therefore, the second case of Lemma 28 must hold, and we have that $M > \epsilon$ and $P > C$. It follows that $P \xrightarrow{\tau} R$, and therefore that $P \to Q$. □

Lemma 57 *If $M.P \xrightarrow{N} P'$ then either:*

(1) $M > N.N'$ *and* $P' \equiv N'.P$, *or*

(2) $M > \epsilon$ *and* $P \xrightarrow{N} P'$.

Proof By definition, $M.P \xrightarrow{N} P'$ implies that $M.P > (\nu\vec{p})\langle N.P_1\rangle P_2$ with $P' = (\nu\vec{p})(P_1 \mid P_2)$ and $fn(N) \cap \{\vec{p}\} = \varnothing$. By Lemma 28, one of two cases arises. In the first case, $M > N.N'$, $(\nu\vec{p})\langle N.P_1\rangle P_2 = (\nu)\langle N.R\rangle\mathbf{0}$, and $R \equiv N'.P$. So $\vec{p} = \varnothing$, $P_1 = R$, and $P_2 = \mathbf{0}$. Therefore, $P' \equiv R \mid \mathbf{0} \equiv N'.P$. In the second case, $M > \epsilon$ and $P > (\nu\vec{p})\langle N.P_1\rangle P_2$. By (Trans Cap), $P \xrightarrow{N} (\nu\vec{p})(P_1 \mid P_2) = P'$. □

Lemma 58 *Consider any closed P and P' such that $P \sim P'$. If $H\{M.P\} \Downarrow n$ then $H\{M.P'\} \Downarrow n$.*

Proof By induction on the derivation of $H\{M.P\} \Downarrow n$.

(Conv Exh) Here $H\{M.P\} \downarrow n$, and we are to show that $H\{M.P'\} \Downarrow n$. By Proposition 14, either (1) $H\{Q\} \downarrow n$ for all Q, or (2) $M.P \downarrow n$, and for all Q, $Q \downarrow n$ implies that $H\{Q\} \downarrow n$. In case (1), we immediately get that $H\{M.P'\} \downarrow n$, and therefore obtain $H\{M.P'\} \Downarrow n$ by (Conv Exh). In case (2), $M.P \downarrow n$ implies that $M.P > (\nu\vec{r})\langle n[R_1]\rangle R_2$ with $n \notin \{\vec{r}\}$ by Proposition 7. By Lemma 28, $M.P > (\nu\vec{r})\langle n[R_1]\rangle R_2$ implies that $M > \epsilon$ and $P > (\nu\vec{r})\langle n[R_1]\rangle R_2$. (The first clause of Lemma 28 cannot apply since the prime of the concretion $(\nu\vec{r})\langle n[R_1]\rangle R_2$ is an ambient and not an action.) By Proposition 7 and (Conv Exh), we get that $P \Downarrow n$. Since $P \sim P'$, it follows that $P' \Downarrow n$. So there is P'' such that $P' \rightarrow^* P''$ and $P'' \downarrow n$. We have $H\{P'\} \rightarrow^* H\{P''\}$, and $H\{P''\} \downarrow n$, by the property of H obtained from Proposition 14 above. These two facts imply that $H\{P'\} \Downarrow n$.

(Conv Red) Here $H\{M.P\} \rightarrow R$ and $R \Downarrow n$. By Theorem 15, one of the following cases must hold:

(Act Proc) Then $M.P \rightarrow R'$ with $R \equiv H\{R'\}$. By Lemma 56, we have that $M > \epsilon$ and $P \rightarrow R'$. If $M > \epsilon$, then $H\{M.P\} \equiv H\{P\}$, so $H\{P\} \Downarrow n$. Since $P \sim P'$, $H\{P\} \Downarrow n$ implies that $H\{P'\} \Downarrow n$. From $M > \epsilon$, we get that $H\{M.P'\} \equiv H\{P'\}$, and therefore that $H\{M.P'\} \Downarrow n$.

(Act Har) Then $H \rightarrow H'$ with $R \equiv H'\{M.P\}$. By Lemma 2, $R \equiv H'\{M.P\}$ implies that $H'\{M.P\} \Downarrow n$ with the same depth of inference as $R \Downarrow n$. By induction hypothesis, we get $H'\{M.P'\} \Downarrow n$ too. From $H \rightarrow H'$ we get that $H\{M.P'\} \rightarrow H'\{M.P'\}$, and hence that $H\{M.P'\} \Downarrow n$.

(Act Inter) Then there are H' and $\vec{r}$ with $\{\vec{r}\} \cap fn(M.P) = \varnothing$, and one of several cases holds. We consider just one; the others follow by similar arguments.

(Inter In) Here $H \equiv (\nu\vec{r})H'\{m[- \mid R'] \mid n[R'']\}$, $M.P \xrightarrow{in\, n} P'$, and and $R \equiv (\nu\vec{r})H'\{n[m[P' \mid R'] \mid R'']\}$. By Lemma 57, $M.P \xrightarrow{in\, n} P'$ implies that one of two cases must hold.

In the first case, $M > in\, n.N'$ and $P' \equiv N'.P$. Here, $M.P' \xrightarrow{in\, n} N'.P'$, and therefore we have:

$$\begin{array}{rcl} H\{M.P'\} & \xrightarrow{\tau} & (\nu\vec{r})H'\{n[m[N'.P' \mid R'] \mid R'']\} \\ R & \equiv & (\nu\vec{r})H'\{n[m[N'.P \mid R'] \mid R'']\} \end{array}$$

By induction hypothesis, $R \Downarrow n$ and Lemma 2 implies that

$$(\nu\vec{r})H'\{n[m[N'.P' \mid R'] \mid R'']\} \Downarrow n$$

and therefore that $H\{M.P'\} \Downarrow n$.

In the second case, $M > \epsilon$ and $P \xrightarrow{in\, n} P'$. We have $H\{M.P\} \equiv H\{P\}$, and $H\{M.P'\} \equiv H\{P'\}$. Therefore $H\{M.P\} \Downarrow n$ and $P \sim P'$ imply that $H\{M.P'\} \Downarrow n$. □

Proposition 59 *If $P \sim P'$ then $M.P \sim M.P'$.*

Proof Consider any substitution σ with $dom(\sigma) = fv(M.P) \cup fv(M.P')$, and any closed harness H and any name m. By Lemma 58, we get that $H\{M\sigma.P\sigma)\} \Downarrow m$ if and only if $H\{M\sigma.P'\sigma)\} \Downarrow m$. Hence, $M.P \sim M.P'$. □

Lemma 60 *If $H\{P\} \Downarrow n$ then $H\{P \mid Q\} \Downarrow n$.*

Proof Suppose $H\{P\} \Downarrow n$. Let $H' = H\{P \mid -\}$. We have that $H\{P\} \equiv H\{P \mid \mathbf{0}\} = H'\{\mathbf{0}\}$. Hence, by Lemma 2, $H\{P\} \Downarrow n$ implies $H'\{\mathbf{0}\} \Downarrow n$. By Lemma 18, this implies $H'\{Q\} \Downarrow n$, which is to say that $H\{P \mid Q\} \Downarrow n$. □

Proposition 61 *If $P \sim P'$ then $!P \sim !P'$.*

Proof Consider any substitution σ with $dom(\sigma) = fv(!P) \cup fv(!P')$, that is, $dom(\sigma) = fv(P) \cup fv(P')$. Consider any closed harness H and any name n. Suppose that $H\{(!P)\sigma\} \Downarrow n$. By Lemma 49, there is k such that $H\{(P\sigma)^k\} \Downarrow n$. By Proposition 51, $(P\sigma)^k \sim (P'\sigma)^k$. Therefore, $H\{(P\sigma)^k\} \Downarrow n$ implies $H\{(P'\sigma)^k\} \Downarrow n$. By Lemma 60, this implies $H\{(P'\sigma)^k \mid !(P'\sigma)\} \Downarrow n$. Since $H\{!P'\sigma\} \equiv H\{(P'\sigma)^k \mid !(P'\sigma)\}$, it follows that $H\{!P'\sigma\} \Downarrow n$, which is to say, $H\{(!P')\sigma\} \Downarrow n$. By symmetric reasoning, $H\{(!P')\sigma\} \Downarrow n$ implies $H\{(!P)\sigma\} \Downarrow n$. □

Lemma 62 *Consider any P and P' such that $P \sim P'$ and $fv(P) \cup fv(P') \subseteq \{x\}$. If $H\{(x).P\} \Downarrow n$ then $H\{(x).P'\} \Downarrow n$.*

Proof By induction on the derivation of $H\{(x).P\} \Downarrow n$.

(Conv Exh) Here $H\{(x).P\} \downarrow n$. By Proposition 14, either $H\{Q\} \downarrow n$ for all Q, or $(x).P \downarrow n$. In the first case, we get $H\{(x).P'\} \downarrow n$. In the second case, Proposition 7 implies that $(x).P$ hardens to a concretion whose prime is an ambient. This is impossible, so the second case cannot arise.

(Conv Red) Here $H\{(x).P\} \rightarrow R$ and $R \Downarrow n$. By Theorem 15, one of the following cases must hold:

(Act Proc) Then $(x).P \rightarrow R'$ with $R \equiv H\{R'\}$. This case cannot arise, since $(x).P$ has no τ-transitions.

(Act Har) Then $H \rightarrow H'$ with $R \equiv H'\{(x).P\}$. By Lemma 2, $R \equiv H'\{(x).P\}$ implies that $H'\{(x).P\} \Downarrow n$ with the same depth of inference as $R \Downarrow n$. By induction hypothesis, we get $H'\{(x).P'\} \Downarrow n$ too. From $H \rightarrow H'$ we get that $H\{(x).P'\} \rightarrow H'\{(x).P'\}$, and hence that $H\{(x).P'\} \Downarrow n$.

(Act Inter) Then $H \bullet (x).P \rightsquigarrow R$. By analysing the rules of interaction, $H \bullet (x).P \rightsquigarrow R$ can only be derived using (Inter Input) given that $H \equiv (\nu\vec{r})H'\{- \mid \langle M\rangle\}$, $(x).P > (\nu\vec{p})\langle (x).P_1\rangle P_2$, and $R \equiv (\nu\vec{r})H'\{(\nu\vec{p})(P_1\{x{\leftarrow}M\} \mid P_2)\}$, with $\{\vec{p}\} \cap \mathit{fn}(M) = \varnothing$ and $\{\vec{r}\} \cap \mathit{fn}(P) = \varnothing$. From $(x).P > (\nu\vec{p})\langle (x).P_1\rangle P_2$, it follows that $\vec{p} = \varnothing$, $P_1 = P$, $P_2 = \mathbf{0}$. Therefore, $R \equiv (\nu\vec{r})H'\{P\{x{\leftarrow}M\}\}$. We have that $(\nu\vec{r})H'\{P\{x{\leftarrow}M\}\} \Downarrow n$. By assumption, this implies that $(\nu\vec{r})H'\{P'\{x{\leftarrow}M\}\} \Downarrow n$. Now, $H\{(x).P'\} \equiv (\nu\vec{r})H'\{(x).P' \mid \langle M\rangle\} \rightarrow (\nu\vec{r})H'\{P'\{x{\leftarrow}M\}\}$. Therefore, $H\{(x).P'\} \Downarrow n$. □

Proposition 63 *If $P \sim P'$ then $(x).P \sim (x).P'$.*

Proof Consider any substitution σ with $\mathit{dom}(\sigma) = \mathit{fv}((x).P) \cup \mathit{fv}((x).P')$, that is, $\mathit{dom}(\sigma) = (\mathit{fv}(P) \cup \mathit{fv}(P')) - \{x\}$. From $P \sim P'$ it follows that $P\sigma \sim P'\sigma$ and that $\mathit{fv}(P\sigma) \cup \mathit{fv}(P'\sigma) \subseteq \{x\}$. Consider any closed harness H and any name n. By Lemma 62, we get $H\{(x).P\sigma)\} \Downarrow n$ if and only if $H\{(x).P'\sigma)\} \Downarrow n$. Hence, $(x).P \sim (x).P'$. □

Proposition 64 *If $P \sim P'$ then $\mathcal{C}(P) \sim \mathcal{C}(Q)$.*

Proof Combine Proposition 50, Proposition 51, Proposition 53, Proposition 55, Proposition 59, Proposition 61, and Proposition 63. □

We end by proving that the relations $P \sim Q$ and $P \simeq Q$ are one.

Proposition 65 *If $P \sim Q$ then $P \simeq Q$.*

Proof We must show for all names n and contexts $\mathcal{C}$ with $\mathcal{C}(P)$ and $\mathcal{C}(Q)$ closed, that $\mathcal{C}(P) \Downarrow n \Leftrightarrow \mathcal{C}(P) \Downarrow n$, assuming that $P \sim Q$. By Proposition 64, $P \sim Q$ implies that $\mathcal{C}(P) \sim \mathcal{C}(Q)$. Therefore $\mathcal{C}(P) \Downarrow n \Leftrightarrow \mathcal{C}(P) \Downarrow n$ follows from the definition of $\mathcal{C}(P) \sim \mathcal{C}(Q)$, given that $\mathcal{C}(P)$ and $\mathcal{C}(Q)$ are closed. □

To show the converse implication, we need the following combinator.

A substitution combinator: *subst x M P*

$$\mathit{subst}\ x\ M\ P \triangleq (\nu m)(\nu n)(\mathit{open}\ n \mid m[\langle M\rangle \mid (x).n[\mathit{out}\ m.\mathit{open}\ m.P]])$$
$$\text{for } \{m,n\} \cap \mathit{fn}(M.P) = \varnothing$$

Lemma 66 *For all P and M, $\mathit{subst}\, x\ M\ P \sim P\{x{\leftarrow}M\}$.*

Proof Consider the processes defined as follows, with $\{m,n\} \cap \mathit{fn}(M.P) = \varnothing$.

$$\begin{aligned}
R_1 &\triangleq (\nu m)(\nu n)(\mathit{open}\, n \mid m[\langle M\rangle \mid (x).n[\mathit{out}\, m.\mathit{open}\, m.P]]) \\
R_2 &\triangleq (\nu m)(\nu n)(\mathit{open}\, n \mid m[n[\mathit{out}\, m.\mathit{open}\, m.P\{x{\leftarrow}M\}]]) \\
R_3 &\triangleq (\nu m)(\nu n)(\mathit{open}\, n \mid n[\mathit{open}\, m.P\{x{\leftarrow}M\}] \mid m[]) \\
R_4 &\triangleq (\nu m)(\mathit{open}\, m.P\{x{\leftarrow}M\} \mid m[]) \\
R_5 &\triangleq P\{x{\leftarrow}M\}
\end{aligned}$$

We omit the details, but using the activity lemma we can show that $R_i \sim R_{i+1}$ for $i \in 1..4$, much as in the proof of Lemma 19. By transitivity, we obtain $R_1 \sim R_5$, that is, $\mathit{subst}\, x\ M\ P \sim P\{x{\leftarrow}M\}$. □

Lemma 67 *If $P \simeq Q$ then $P\{x{\leftarrow}M\} \simeq Q\{x{\leftarrow}M\}$.*

Proof From $P \simeq Q$ it follows that $\mathit{subst} x\, M\, P \simeq \mathit{subst} x\, M\, Q$. By Lemma 66 and Proposition 65, we get that $\mathit{subst}\, x\ M\ P \simeq P\{x{\leftarrow}M\}$ and $\mathit{subst}\, x\ M\ Q \simeq Q\{x{\leftarrow}M\}$. Combining these equations yields $P\{x{\leftarrow}M\} \simeq Q\{x{\leftarrow}M\}$. □

Proposition 68 *If $P \simeq Q$ then $P \sim Q$.*

Proof Suppose $P \simeq Q$. Consider any substitution σ with $\mathit{dom}(\sigma) = \mathit{fv}(P) \cup \mathit{fv}(Q)$, and any closed harness H and name n. By Lemma 67, $P \simeq Q$ implies that $P\sigma \simeq Q\sigma$. Since $\simeq$ is a congruence, Proposition 1, we get that $H\{P\sigma\} \simeq H\{Q\sigma\}$. By definition of $H\{P\sigma\} \simeq H\{Q\sigma\}$, the fact that $H\{P\sigma\}$ and $H\{Q\sigma\}$ are closed implies that $H\{P\sigma\} \Downarrow n \Leftrightarrow H\{Q\sigma\} \Downarrow n$. Therefore $P \sim Q$. □

Proof of Theorem 12 *For all processes P and Q, $P \simeq Q$ if and only if for all substitutions σ with $\mathit{dom}(\sigma) = \mathit{fv}(P) \cup \mathit{fv}(Q)$, and for all closed harnesses H and names n, that $H\{P\sigma\} \Downarrow n \Leftrightarrow H\{Q\sigma\} \Downarrow n$.*

Proof By definition of $P \sim Q$, this is equivalent to showing that $P \simeq Q$ if and only if $P \sim Q$, for all P and Q, which follows from Proposition 65 and Proposition 68. □