Weak Bisimulations for a Calculus of Broadcasting Systems

M. Hennessy, J. Rathke
University of Sussex

March 1 , 1995

Abstract

A theory of weak bisimulation equivalence is developed for the broadcast calculus *CBS*. The exact notion of bisimulation we study is justified by a characterisation in terms of a version of barbed bisimulations. We then give two syntactic characterisations of the associated congruence over finite expressions. The first is in terms of a set of equations together with an infinitary proof rule to accommodate input prefixes. The second uses a finitary proof system where the judgements are relative to properties of the data domain.

1 Introduction

The broadcast calculus, CBS, is a value-passing process calculus where process intercommunication is achieved by the broadcasting of values. The main operators of the language are

- $x?T$ - receive a value v and proceed as $T[v/x]$
- $e!T$ - broadcast the value of the expression e and proceed as T
- $T \mid U$ - run processes T and T

meaning in all evaluations which satisfy the boolean constraint b the evaluation of T is semantically equivalent to that of U. Here the proof rules depend on deductions which can be made in an independent proof system for the data domain.

Here we carry out a similar programme of research, but now under the assumption that the moves $\tau!$ are internal and therefore invisible; in the terms of [5] we develop a *weak* semantic theory for CBS. Once more we justify our choice of equivalence using a *weak* version of barbed bisimulation and in this case it coincides with a semantic equivalence previously suggesed in [8]. We then go on as in [4] and give two different proof theoretic characterisations of the associated congruence over finite processes; one over closed terms which requires an infinitary rule and one over open terms which is relative to an independent proof system for the data domain.

We now outline the remainder of the paper. In section 2 we give the syntax of the particular version of CBS we study. It is similar to that of [8] except that the input prefix $x?T$ is replaced by the input guard $x \in S?T$ where S can be any subset of values. We then give an operational semantics in terms of a labelled transition systems and define *weak barbed bisimulation equivalence.* Finally we characterise the largest CBS congruence contained in this equivalence using the version of weak bisimulation equivalence considered in [8].

In Section 3 we give the infinitary equational characterisation of this congruence over closed finite expressions. We use the equations from [4] which characterise noisy bisimulation equivalence but in addition new equations are required in order to capture the fact that $\tau!$ moves are internal. Unfortunately two of the τ-laws of [5] are unsound in the context of CBS; they are replaced with weaker variants.

In the final section, Section 4, we give the sound and complete finitary proof system, relative to an adequate theory of the data domain. Here we follow closely the approach of [3], and although the technical details are somewhat complicated, we simply adapt the techniques of [4] to take into account the internal moves $\tau!$.

2 Syntax and semantics

The language we will use is that of [4] based on CBS+ [8]. It is a CCS variant in which the traditional handshaking form of communication is replaced by the broadcasting of values. A BNF grammar describing the syntax of the language is

$$T ::= \mathbf{O} \mid e!T \mid x \in S?T \mid b \gg T \mid \sum_{i \in I} T_i \mid T|T \mid T_{(f,g)} \mid A(\tilde{e}).$$

where $e \in ValExp$, a set of data expressions, $x \in Var$, a set of variables, $b \in BoolExp$, a set of boolean expressions and S ranges over subsets of a predefined set of values Val. We do not give a specific syntax for these expressions but we will assume that $ValExp$ contains at least the set of values $Val \cup \{\tau\}$ (where τ is a distinguished value not appearing in Val) and that $BoolExp$ contains the expressions $e = e'$ and $x \in S$ for every $e, e' \in ValExp, x \in Var$ and $S \subseteq Val$. In addition we assume that *evaluations*, functions ρ from Var to Val, can be lifted to $VarExp$ and $BoolExp$ in a straightforward manner. We denote the value of a closed (having no occurences of variables) expression by $[\![e]\!]$; this value is of course independent of ρ. We have substitutions in data and boolean expressions written as $e[e'/x], b[e'/x]$ where the data expression e' is to be substituted for all occurences of x in e, b respectively. Substitution is extended to terms in the obvious way except that only free occurences of variables are substituted; the input prefix $x \in S?T$ binds the variable x in T. This gives rise to the familiar notions of free variables of a term, $fv(T)$, and α-equivalence between terms. We call a term P a *process* or *agent* if P contains no free variables. Certain metavariables will be used, consistent with those of

[4]. $P, Q, \ldots$ will denote closed processes whereas $T, U, \ldots$ will denote arbitrary terms of the language, v ranges over values in Val and w over values in $Val \cup \{\tau\}$.

The process $e!P$ is the process which broadcasts the value of the expression e and then continues to behave like P. Input prefixing is decorated with a set $S \subseteq Val$ which is called the *input guard.* The process $x \in S?T$ may only receive values present in S; upon receipt of such a value v it continues to behave like $T[v/x]$. The boolean guard $b \gg T$ is a data testing operator where b acts like a *boolean guard* to T. In $T_{(f,g)}$ f and g are functions from $Val \cup \{\tau\}$ to $Val \cup \{\tau\}$ such that $f(\tau) = g(\tau) = \tau$ and are used to localise and rename messages. Communication is achieved via the multiway parallel operator $|$. Process constants $A(\tilde{e})$ are used to define recursive processes and we asssume throughout the report that with each constant name, A, we have an associated definition

$$A(\tilde{e}) \overset{def}{=} T_A.$$

The operational semantics for closed terms of the language is presented in Figure 1, where symmetric rules for the choice operator $+$ have been omitted. It is exactly the operational semantics used in [4] which in turn is based on that of [8]; in terms of [6] it is an early operational semantics. The use of the discard transition, written $T \xrightarrow{w:} T$, may be unfamiliar to the reader. This is essentially a negation of the transition $T \xrightarrow{w?} T'$ for some T' (see Lemma 2.1 below) and is used to facilitate the presentation of the semantics for the parallel operator.

The following lemma is imported from [4]. It states a few simple facts about the operational semantics which are used extensively in the subsequent proofs.

Lemma 2.1 *For every agent P*

i if $P \xrightarrow{w:} Q$ then Q is P.

ii $P \xrightarrow{v:} Q$ if and only if there does not exist a Q such that $P \xrightarrow{v?} Q$.

iii $P \xrightarrow{\tau:} P$. □

Weak moves, traditionally denoted by the double arrow, can now be defined as the least relations between closed terms that satisfy the following:

- $P \overset{\varepsilon}{\Longrightarrow} P$
- $P \xrightarrow{\alpha} Q$ implies $P \overset{\alpha}{\Longrightarrow} Q$
- $P \xrightarrow{\tau!} \overset{\alpha}{\Longrightarrow} Q$ implies $P \overset{\alpha}{\Longrightarrow} Q$
- $P \overset{\alpha}{\Longrightarrow} \xrightarrow{\tau!} Q$ implies $P \overset{\alpha}{\Longrightarrow} Q$

where $\alpha \in \{w!, v?, w:\}$. We will occasionally use the notation $P \overset{\tau!\alpha}{\Longrightarrow} Q$ to mean $P \overset{\tau!}{\Longrightarrow} \overset{\alpha}{\Longrightarrow} Q$, and we will define $\hat{\alpha}$ to be ε when $\alpha = \tau!$ and α otherwise.

We turn now to the definition of a *weak* semantic equivalence, which abstracts away from the occurrence of $\tau!$ actions. As in [4] we use the technique of barbed bisimulations [10] to provide us with an appropriate notion of weak bisimulation. In [4] the method provided a novel version of strong bisimulation called noisy bisimulation and it transpires that the congruence associated with weak barbed bisimulation will be characterised by the corresponding weak version of noisy bisimulation.

For any value v let $P \downarrow v$ mean that there exists a P' such that $P \xrightarrow{v!} P'$.

Discard	Input	Output
$\mathbf{O} \xrightarrow{w:} \mathbf{O}$		
$\dfrac{w \notin S}{x \in S?T \xrightarrow{w:} x \in S?T}$	$\dfrac{v \in S}{x \in S?T \xrightarrow{v?} T \quad x \in}$	

Proof. We only outline the proof here as the details are similar to those in [10]. Given a value set Val we extend this to a value set Val^+ defined to be the disjoint union of the sets Val, $Val' \overset{def}{=} \{v' \mid v \in Val\}, \{in, out, c\}$ and $\{d_i \mid i \in N\}$. We define translation functions on $Val^+ \cup \{\tau\}$ as follows:

$$g(w) = \begin{cases} w' & \text{if } w \in Val \\ w & \text{otherwise.} \end{cases}$$

$$f(w) = \begin{cases} \tau & \text{if } w \in Val \cup \{c\} \\ w & \text{otherwise.} \end{cases}$$

$$h(w) = \begin{cases} \tau & \text{if } w = c \\ w & \text{otherwise.} \end{cases}$$

Armed with these we can build a collection of static contexts $C_n[\ \_\ ]$ similar to those in [10]. A full explanation of the construction of Sangiorgi's contexts can be found in his thesis. Ours differ only in that we explicitly translate communicated values into τ actions using the translation functions and we require the use of a distinguished value c which plays the rôle of a private channel for communicating with and incrementing the counter.

We let $+$ denote binary choice and define

$$Count_n \overset{def}{=} d_n!\mathbf{O} + x \in \{c\}?Count_{n+1}$$

and the constant D

$$\begin{aligned} D \overset{def}{=} &\ x \in Val?c!c!(\tau!(g(x)!\mathbf{O} + out!\mathbf{O}) + \tau!D) \\ + &\ \sum_{v \in Val} v!c!c!(\tau!(g(v)!\mathbf{O} + in!\mathbf{O}) + \tau!D) \\ + &\ \tau!d_0!\mathbf{O} \\ + &\ \tau!d_1!\mathbf{O} \end{aligned}$$

The contexts we require then are defined by

$$C_n[\ \_\ ] \overset{def}{=} ([\ \_\ ]_{[id,h]}|D|Count_n)_{[f,id]}.$$

Given these we define a relation $S = \{(R, S) \mid \exists\cup\Rightarrow\not\Rightarrow\mathcal{R}\notin\{\forall\in\notin\in\exists\notin\exists\mathcal{R}\in\in\{\notin\{\forall\mathcal{R}\forall\forall\Rightarrow\Rightarrow\notin\in\Rightarrow|\in\Rightarrow|\in\Rightarrow\Rightarrow\in\{\not\forall$

Definition 2.7 *Observational congruence $=$ is the symmetric relation defined by $P = Q$ if*

- *if* $P \xrightarrow{w!} P'$ *then* $\exists Q' \cdot Q \overset{w!}{\Longrightarrow} Q'$ *and* $P' \approx Q'$
- *If* $P \xrightarrow{v?} P'$ *then* $\exists Q'.Q \overset{v?}{\Longrightarrow} Q'$ *and* $P' \approx Q'$
  or $Q \overset{\tau!v:}{\Longrightarrow} Q'$ *and* $P' \approx Q'$
- *If* $P \xrightarrow{v:} P$ *then* $Q \xrightarrow{v:} Q$

Theorem 2.8 *$P =_{barb} Q$ if and only if $P = Q$.*

Proof. We leave the reader to check that $=$ is preserved by all the operators in CBS and since $P = Q$ trivially implies that $P \approx_{barb} Q$ we conclude that $P = Q$ implies $P =_{barb} Q$.

Conversely, suppose $P =_{barb} Q$. Then $C[P + v_0!\mathbf{O}] \approx_{barb} C[Q + v_0!\mathbf{O}]$ for all static contexts $C[\ \_\ ]$, where v_0 is some distinguished value not in Val. It follows from Proposition 2.6 that $P + v_0!\mathbf{O} \approx Q + v_0!\mathbf{O}$.

We now prove that $P + v_0!\mathbf{O} \approx Q + v_0!\mathbf{O}$ implies $P = Q$. As an example we show $P \xrightarrow{v:} P$ implies $Q \xrightarrow{v:} Q$; the remaining requirements are similar. From $P \xrightarrow{v:} P$ it follows that $P + v_0!\mathbf{O} \xrightarrow{v:} P + v_0!\mathbf{O}$ also. By the hypothesis we know that $Q + v_0!\mathbf{O} \overset{v??}{\Longrightarrow} Q'$ for some $Q' \approx P + v_0!\mathbf{O}$. This means that Q' is $Q + v_0!\mathbf{O}$ as otherwise $Q' \not\xrightarrow{v_0!}$. So we have that $Q + v_0!\mathbf{O} \xrightarrow{v:} Q + v_0!\mathbf{O}$ which in turn implies that $Q \xrightarrow{v:} Q$. □

3 Characterising Observational Congruence over Finite Agents

We present an algebraic characterisation of observational congruence over a class of finite agents. The syntax for this finite sub-language is given by the grammar

$$T ::= \mathbf{O} \mid e!T \mid x \in S?T \mid b \gg T \mid T + T.$$

We have restricted the summation operator Σ_I to binary choice $+$ recursion is not allowed. The extra CBS operators, parallel and translations, can be treated in this language by using a suitable expansion law and coding technique [4], Section 7. We denote the class of agents (closed terms) definable in this sub-language by $\mathcal{FA}$ and we use α, β to range over arbitrary prefixes of the form $e!$ and $s \in S?$.

The algebraic characterisation is in terms of a proof system whose rules are given in Figure 3; it is the standard adaption of an equation proof system to handle a value-passing language. The main non-standard rule is the infinitary proof rule cl-INPUT to deduce judgements about expressions involving input prefixes.

We now discuss the required equations.

[illegible]

I]y I$e!P$ I$x \in S?T$]y IP

Ident: $X + 0 = X$

Idemp: $X + X = X$

Comm: $X + Y = Y + X$

Assoc: $X + (Y + Z) = (X + Y) + Z$

Noisy: $e!(X + x \in S?X) = e!X \quad \text{if } S \cap I(X) = \emptyset$

Pattern: $x \in S?X + x \in S'?X = x \in S \cup S'?X$

Empty: $x \in \emptyset?X = \mathbf{O}$

Tau1: $e!(\tau!X + X) = e!X$

Tau2: $\alpha.(X + \tau!Y) + \alpha.Y = \alpha.(X + \tau!Y)$

Tau3: $X + x \in S?Z + \tau!(Y + x \in S?Z) = X + \tau!(Y + x \in S?Z) \quad \text{if } S \subseteq I(X)$

Tau4: $e!X + \tau!(Y + e!X) = \tau!(Y + e!X)$

Figure 2: Axioms $\mathcal{A}_{cl}$ for weak bisimulation (closed terms)

- $I(b \gg P) = \begin{cases} I(P) & \text{if } [\![b]\!] = \mathbf{tt} \\ \emptyset & \text{otherwise} \end{cases}$

Pattern : $x \in S?X + x \in S'?X = x \in S \cup S'?X.$

Empty : $x \in \emptyset?X = \mathbf{O}.$

As noisy congruence is strictly contained in observational congruence it is clear that we also require these axioms for our present characterisation. In addition to these axioms then we require analogies of the tau laws of CCS:

A1 $\alpha.\tau.P =_{ccs} \alpha.P.$

A2 $\alpha.(P + \tau.Q) + \alpha.Q =_{ccs} \alpha.(P + \tau.Q).$

A3 $P + \tau.P =_{ccs} \tau.P.$

Unfornutately $A1$ and $A3$ are not sound for CBS. We have already seen, for example, that P is not, in general, weakly bisimilar to $\tau!P$ which implies, for example that $0!\tau!P \neq 0!P$. For $A3$ we run into difficulties when P is allowed to recieve any value v, say. For then $\tau!P$ may discard v but $P + \tau!P$ is obliged to receive it. We adopt admissible versions of these axioms. $A1$ simply becomes
  $Tau1 : e!(\tau!X + X) = e!X,$
$A2$ is adapted to
  $Tau2 : \alpha.(X + \tau!Y) + \alpha.Y = \alpha.(X + \tau!Y),$
and $A3$ splits into two axiom schemes[1]

[1]It is possible, for present purposes, to give these two as a single axiom scheme though to be consistent with the sequel we use two.

EQUIV $\dfrac{}{P = P} \quad \dfrac{P = Q}{Q = P} \quad \dfrac{P = Q \quad Q = R}{P = R}$

AXIOM $\dfrac{P = Q \in \mathcal{AX}}{P\rho = Q\rho}$

CONG $\dfrac{P_1 = Q_1 \quad P_2 = Q_2}{P_1 + P_2 = Q_1 + Q_2}$

α-CONV $\dfrac{}{x \in S?T = y \in S?T[y/x]} \quad y \notin fv(T)$

cl-INPUT $\dfrac{\tau!T[v/x] + \tau!U[v/x] = \tau!U[v/x] \quad \text{for every } v \in S}{x \in S?T + x \in S?U = x \in S?U}$

OUTPUT $\dfrac{P = Q, \quad [\![e]\!] = [\![e']\!]}{[\![e]\!]!P = [\![e']\!]!Q}$

BOOL $\dfrac{[\![b]\!] = \mathbf{tt}}{b \gg P = P} \quad \dfrac{[\![b]\!] = \mathbf{ff}}{b \gg P = \mathbf{O}}$

We say a closed term is in *standard form* if it has the form

$$\sum_{i \in I_!} e_i!T_i + \sum_{i \in I_?} x_i \in S_i?T_i$$

for some finite indexing sets $I_!$ and $I_?$ such that S_i is non-empty for each $i \in I_?$

Theorem 3.5 *(Decomposition) Let $S = I(Q) - I(P)$ and $S' = I(P) - I(Q)$. $P \approx Q$ iff one of the following holds:*

(i) $P + x \in S?P = Q + x \in S'?Q$ *and when* S *and* S' *are both non-empty there exist* P', Q' *such that* $d(P') < d(P), d(Q) < d(Q')$ *and* $P' \approx P, Q' \approx Q$.

(ii) $P + x \in S?P + \tau!P = Q + x \in S'?Q$ *and when* S' *is non-empty there exist* P', Q' *such that* $d(P') < d(P)$, $d(Q') < d(Q)$ *and* $P' \approx P$, $Q' \approx Q$.

(iii) $P + x \in S?P = Q + x \in S'?Q + \tau!Q$ *and when* S *is non-empty there exist* P', Q' *such that* $d(P') < d(P)$, $d(Q') < d(Q)$ *and* $P' \approx P$, $Q' \approx Q$.

Proof. The 'if' direction is standard. So suppose $P \approx Q$.

This can be inferred from the rule cl-INPUT if we can prove for each $v \in S_l^j$

$$\mathcal{A}_{cl} \vdash_{cl} \tau!T_j[v/x] + \tau!U_l[v/x] = \tau!U_l[v/x].$$

So let us fix a particular $v \in S_l^j$ and see how this can be inferred. We know that $T_j[v/x] \approx Q_l^v$ so from this we will show that

$$\mathcal{A}_{cl} \vdash_{cl} \tau!T_j[v/x] = \tau!Q_l^v$$

and the result will follow by the Derivation Lemma and $Tau2$.

For convenience let P, Q denote $T_j[v/x]$, Q_l^v respectively. We now apply Theorem 3.5 to get one of three possibilities

(i) $P + x \in U?P = Q + x \in V?Q$

(ii) $P + x \in U?P + \tau!P = Q + x \in V?Q$

(iii) $P + x \in U?P = Q + x \in V?Q + \tau!Q$

where $U = I(Q) - I(P)$ and $V = I(P) - I(Q)$. We show how to deal with case (iii) and leave cases (i) and (ii) to the reader. We have two eventualities to consider.

1. $U = \emptyset$
   Here we have $P = Q + x \in V?Q + \tau!Q$ and we can use induction to obtain $\mathcal{A}_{cl} \vdash_{cl} \tau!P = \tau!(Q + x \in V?Q + \tau!Q)$. Now we can apply the *Noisy* scheme to obtain

   $$\mathcal{A}_{cl} \vdash_{cl} \tau!P = \tau!(Q + x \in V?Q + \tau!(Q + x \in V?Q))$$

   from which $\mathcal{A}_{cl} \vdash_{cl} \tau!P = \tau!(Q + x \in V?Q)$ follows by *Tau1*. Another appplication of *Noisy* gives the required result.

2. $U \neq \emptyset$
   Here we have $P + x \in U?P = Q + x \in V?Q + \tau!Q$ and in this case we cannot apply induction immediately as the combined depth of the terms has not decreased. But Thereom 3.5 tells us that there exists P', Q' such that $d(P') < d(P)$ and $d(Q') < d(Q)$ such that $P' \approx P$ and $Q' \approx Q$. Suppose without loss of generality that $d(P) \leq d(Q)$.
   Then,)hat∃∃∈⇒|R∈{∈∃∃∈ ⇒|R{≠|⇒∈∃∃∈⇒|R∀∃∀|∀⇒∄⇒|∪{∀∪⇒∉⇒R∈{∄∈∀A⇒|R∈∈∈{∄∃∈∀∀⇒|

$\in U?$ $U + x \in$ app22N08.6790d(Q)Tj//R2320.24Tf7.43922.08010Td.0Td624Tf11.2/R1360.26801Tin13.68014(turn131960

4 A Finitary Proof System

We now show that the proof system of the previous section can be improved upon by removing infinitary inference rules. This improvement brings the proof system out of the realm of theoretical proof machines by making its implementation a realistic task. The proof system we develop is for observational congruence over open terms of the finite sublanguage presented in Section 3. It follows closely the corresponding proof systems given in [3, 4].

The judgements of the proof system are now decorated with boolean expressions:

$$b \rhd T = U$$

and intuitively this is meant to denote that $T\rho = U\rho$ for every evaluation ρ such that $\rho(b) = \mathbf{tt}$. The inference rules for the proof system, borrowed directly from [3, 4] are given in Figure 4. We also borrow the notation $\rho \models b$ to mean $[\![b\rho]\!] = \mathbf{tt}$ and $b \models b'$ to mean that $\rho \models b$ implies $\rho \models b'$.

We state a few simple facts about the proof system which we make use of in the sequel; they show how booleans can be manipulated in the proof system.

Proposition 4.1

(i) $b \models b'$ *implies* $\vdash b \rhd T = b' \gg T$

(ii) $\vdash b \gg (T + U) = (b \gg T) + (b \gg U)$

(iii) $\vdash (b \gg T) + (b' \gg T) = b \vee b' \gg T$

(iv) $b \models b'$ *and* $\vdash T = T + b' \gg U$ *implies* $\vdash T = T + b \gg U$. □

We use more or less the same equations as in the proof system for closed terms. There are two exceptions, *Noisy* and *Tau3*. These are in fact axiom schemes and are defined in terms of the sets $I(P)$ for closed expressions P. In order to generalise these axiom schemes to open terms we need to extend the function I to open terms. We follow the approach taken in [4] and relativise it to a boolean world, defining $I(b, T)$, the set of values which the term T may receive when T is instantiated as an agent by an evaluation ρ such that ρ {

EQUIV $\dfrac{}{\mathbf{tt} \rhd T = T} \quad \dfrac{b \rhd T = U}{b \rhd U = T} \quad \dfrac{b \rhd T = U \quad b \rhd U = V}{b \rhd T = V}$

AXIOM $\dfrac{T = U \in \mathcal{AX}}{\mathbf{tt} \rhd T\rho = U\rho}$

CONG $\dfrac{b \rhd T_1 = U_1 \quad b \rhd T_2 = U_2}{b \rhd T_1 + T_2 = U_1 + U_2}$

α-CONV $\dfrac{}{\mathbf{tt} \rhd x \in S?T = y \in S?T[y/x]} \quad y \notin fv(T)$

Discard	Input	Output
$\mathbf{O} \xrightarrow{\mathtt{tt}, Val:} \mathbf{O}$		
$x \in S?T \xrightarrow{\mathtt{tt}, Val-S:} x \in S?T$	$y \notin fv(x \in S?T)$	

- $T^{b',e!}$

Proof. Let $B_1 = \{b \wedge b_K \mid K \subseteq I_?\}$ and $B_2 = \{b \wedge b_L \mid L \subseteq J_?\}$ where $I_?$ and $J_?$ are indexing sets of the standard forms T and U respectively. We let B' be the b-partition $\{b_1 \wedge b_2 \mid b_1 \in B_1,\ b_2 \in B_2\}$. It is clear that this partition is

Case $T \overset{b_1,\tau!}{\Longrightarrow} U \overset{b_2,x\in S'?}{\longrightarrow} T'$.

Suppose that $U_? \equiv \sum_{I_?} b_i \gg x_i \in S_i?U_i$. We let

$$B_u = \{b \wedge b_K \mid K \subseteq I_?\}.$$

Clearly then B_u is a U-uniform partition of b. Choose any $b_u(= b \wedge b_K) \in B_u$. We know that $b_u \models b \models b_2$ so b_2 must be equal to some b_{i_0} for some $i_0 \in K$. This means that $S' = S_{i_0} \subseteq I(b_u, U)$. Therefore by induction we get

$$\mathcal{A}_{op} \vdash U = U + b_u \gg x \in S'?T'.$$

This is true for each $b_u \in B_u$ so we can add to get

$$\mathcal{A}_{op} \vdash U = U + \sum_{B_u} b_u \gg x \in S'?T'.$$

Thus by manipulating the boolean guards, remembering that B_u is a b partition, we get

$$\mathcal{A}_{op} \vdash U = U + b \gg x \in S'?T'$$

whence

$$\mathcal{A}_{op} \vdash U = U + b \gg x \in S?T'.$$

Using part (i) we know that

$$\mathcal{A}_{op} \vdash T = T + b_1 \gg \tau!(U + b \gg x \in S?T').$$

Recall that $b \models b_1$, b is T-uniform and $S \subseteq I(b,T)$ so we can apply *Op-Tau3*$^{\gg}$ to get the result.

(iii) We assume that T is a standard form. We know that $T \overset{b',\tau!S':}{\Longrightarrow} T'$ so suppose

$$T \overset{b_1,\tau!}{\Longrightarrow} U \overset{b_2,S':}{\longrightarrow} U \overset{b_3,\varepsilon}{\Longrightarrow} T'$$

where $b' = b_1 \wedge b_2 \wedge b_3$. Suppose also that $U_? \equiv \sum_{I_?} b_i \gg x \in S_i?U_i$. Then

$$b_2 = \bigwedge_{j\in J} \neg b_j \text{ and } S' = \bigcap_{j\in I_?-J} (Val - S_j)$$

for some discard index $J \subseteq I_?$. We let $B_u = \{b \wedge b_K \mid K \subseteq I_?\}$ be a U-uniform, b partition and observe that whenever $j \in K \cap J$ we have that $b \wedge b_K \models b_j$ and $b \wedge b_K \models b_2 \models \neg b_j$. Reading this contrapositively we have that $b \wedge b_K \neq \mathbf{ff}$ implies $K \cap J = \emptyset$.

Our intention is to prove

$$\mathcal{A}_{op} \vdash b \wedge b_K \rhd \tau!U = \tau!(U + x \in S?U)$$

by applying axiom *Op-Noisy* (or ABSURD when $b \wedge b_K = \mathbf{ff}$) to U for each $b \wedge b_K$. In order to do this we need to show that $S \cap I(b \wedge b_K, U) = \emptyset$ whenever $b \wedge b_K \neq \mathbf{ff}$.

Suppose then that $b \wedge b_K \neq \mathbf{ff}$ and suppose for contradiction that $v \in S \cap I(b \wedge b_K, U)$. This means that $v \in S$ and $v \in S_{j_0}$ for some $j_0 \in K$. But $v \in S$ implies that $v \in S' = \bigcap_{j\in I_?-J}(Val - S_j)$, that is $v \notin S_j$ for each $j \in I_? - J$. Therefore $j_0 \notin I_? - J$ and we conclude that $j_0 \in J$, which contradicts $K \cap J = \emptyset$.

We can now apply axiom *Op-Noisy* (ABSURD) for each $b \wedge b_K$ in B_u and then use CUT to obtain

$$\mathcal{A}_{op} \vdash b \rhd \tau!U = \tau!(U + x \in S?U).$$

Boolean manipulation and part (i) gives

$$\mathcal{A}_{op} \vdash T = T + b \gg \tau!(U + b \gg x \in S?U).$$

So an appication of axiom *Op-Tau3*$^{\gg}$ yields

$$\mathcal{A}_{op} \vdash T = T + b \gg x \in S?U.$$

The result follows easily now; if U is T' we are done, otherwise we use part (i) to give

$$\mathcal{A}_{op} \vdash T = T + b \gg x \in S?(U + \tau!T')$$

and apply axiom *Tau2* to finish. □

Theorem 4.7 *(Completeness)*

$$T =^b U \textit{ implies } \mathcal{A}_{op} \vdash b \rhd T = U.$$

Proof. We assume standard forms

$$\sum_{i \in I_!} c_i \gg e_i!T_i + \sum_{i \in I_?} c_i \gg x_i \in S_i?T_i$$

and

$$\sum_{j \in J_!} d_j \gg e_i!U_j + \sum_{j \in J_?} d_j \gg x_j \in S_j?U_j$$

for T and U respectively. We modify these forms in the following way: Suppose $z \notin fv(b, T, U)$. For each $i \in I_?$ we have that $T \overset{c_i, z \in S_i?}{\longrightarrow} T_i[z/x_i]$. Since $T =^b U$ we know that there exists a matching $b \wedge c_i \wedge z \in S_i$-partition, B. Because $z \notin fv(b, c_i)$ we know that each element of B is logically equivalent to something of the form $b' \wedge z \in S_{i_k}$ (for some indexing set K) where $\bigvee b' \equiv b \wedge c_i$ and $\bigcup S_{i_k} = S_i$. We use the axiom *Pattern* to decompose the summand $x_i \in S_i?T_i$ of T into the sum $\sum_{k \in K} x_i \in S_{i_k}?T_i$ and we distribute c_i across this sum. We repeat this for each $i \in I_?$ and also for U.

Having done this T and U enjoy the property that whenever $T \overset{c_i, x \in S_i}{\longrightarrow} T_i$ there exists a $b \wedge c_i \wedge x \in S_i$-partition, B, such that for each $b' \in B$ there exists a d, S, U' such that $U \overset{d, x \in S?}{\Longrightarrow} U'$ or $U \overset{d, \tau!S:}{\Longrightarrow} U'$ with $b' \models d$, $S_i \subseteq S$ and $T_i \approx^{b'} U'$. Moreover given any such partition we can transform it into a U-uniform partition by defining

$$B_u = \{ b' \wedge d_K \mid b' \in B,\ K \subseteq J_? \}.$$

It is sufficient, due to symmetry, to prove for every transition $T \overset{b', \alpha}{\longrightarrow} T'$ that

$$\mathcal{A}_{op} \vdash b \rhd b' \gg \alpha.T' + U = U$$

where α is of the form $e!$ or $x \in S?$ We show how to deal with the latter, the former being slightly easier.

Fix $i \in I_?$ and consider $T \overset{c_i, z \in S_i?}{\longrightarrow} T_i[z/x_i]$. We know that there exists a U-uniform, $b \wedge c_i \wedge z \in S_i$-partition, B_u such that each $b_u \in B_u$ is of the form $b' \wedge z \in S_i$ where the $\{b'\}$ form a $b \wedge c_i$ partition. Furthermore, each b' is of the form $b'_0 \wedge d_K$ for some $K \subseteq J_?$. For each such b_u

We know that $b' \models c_i$ and therefore $b^* \not\models \neg c_i$. This means that i is not in the discard index of $T \overset{b^*, S^*:}{\longrightarrow} T$ which in turn means that $S_i \subseteq (Val - S^*)$. But $Val - S^* = Val - S_{dc} = \bigcup_{j \in K} S_i = I(b', U)$ so we have $S_i \subseteq I(b', U)$.

We also fulfil our obligation in proving

$$\mathcal{A}_{op} \vdash b_u \rhd c_i \gg \tau!T_i[z/x_i] + b' \gg \tau!U' = b' \gg \tau!U'.$$

For convenience let T' denote $T_i[z/x_i]$. We know that $T' \approx^{b_u} U'$ so we can apply the Decomposition Theorem 4.5 to obtain a b_u-partition, B' which is both T' and U'-uniform such that $b =$

References

[1] E. Best, editor. *Proceedings CONCUR 93,* Hildesheim, volume 715 of *Lecture Notes in Computer Science.* Springer-Verlag, 1993.

[2] M. Hennessy and H. Lin. Symbolic bisimulations. Technical Report 1/92, University of Sussex, 1992.

[3] M. Hennessy and H. Lin. Proof systems for message-passing process algebras. In Best [1], pages 202–216.

[4] M. Hennessy and J. Rathke. Strong bisimulations for a calculus of broadcasting systems. Computer Science Report 1/95, University of Sussex, 1995.

[5] R. Milner. *Communication and Concurrency.* Prentice-Hall International, Englewood Cliffs, 1989.

[6] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, Part I + II. *Information and Computation*, 100(1):1–77, 1992.

[7] K.V.S. Prasad. A calculus of broadcast systems. In *TAPSOFT 91 Volume 1: CAAP.* Springer Verlag, 1991.

[8] K.V.S. Prasad. A calculus of value broadcasts. Technical report, Dept. of Computer Science, Chalmers, 1992.

[9] K.V.S. Prasad. Programming with broadcasts. In Best [1].

[10] D. Sangiorgi. *Expressing Mobility in Process Algebras: First-Order and Higher-Order Paradigms.* PhD thesis, University of Edinburgh, 1993.