Errata for
The Fusion Calculus: Expressiveness and Symmetry in Mobile Processes

Björn Victor

1 Weak barbed congruence

Theorem 4.19 of Chapter 4, page 46 in the thesis, stating that weak barbed congruence coincides with weak hyperequivalence, is not valid in general, but only for a certain subclass of fusion calculus agents. In the following we (1) pinpoint the error in the proof of Lemma 4.20 and present some counterexamples, (2) define a subclass of the fusion calculus for which Lemma 4.20 holds and prove this fact, (3) discuss the proof of Lemma 4.18 (this proof is omitted in the thesis by reference to Lemma 4.20), and (4) discuss the impact of the error.

1.1 Demonstration of the problem

The error is in the proof of Lemma 4.20, line 16 on page 47, where the conclusion "This gives $\mathrm{obj}(\alpha) = \tilde{w}$, where $\tilde{x} \subseteq \tilde{w}$ is fresh" is incorrect since Q' may fuse names in $\tilde{x}$, making the observations of $X(\tilde{y}, \tilde{z})$ match those of the corresponding term in S'.

For the fusion calculus weak hyperequivalence is strictly finer than weak barbed congruence, as witnessed by the following example, due to Yuxi Fu:

$$(x)ux\,.\,\{x = z\} \;\underset{\not\approx}{\overset{\approx_b}{}}\; (x)ux\,.\,\{x = z\} + uz$$

It is clear that the agents are not weakly hyperequivalent, since the RHS, call it P, can perform a uz transition which cannot be matched by the LHS, call it Q. Nevertheless, they *are* weak barbed congruent. They have the same observations, namely u. The only possibility for P and Q to be weakly barbed *in*congruent is if there were a context C such that $C[P]$ has a reduction, which cannot be simulated by $C[Q]$, or vice versa. This reduction must then emanate from the term uz in P. Therefore the context must have a parallel component R such that $R \equiv \overline{u}w\,.\,R' + R''$ for some w, and $C[\cdot] \equiv (w)C'[\cdot \mid R]$. (A completely symmetric argument follows from the context $(z)C'[\cdot \mid R]$.) The reduction in question emanates from

$$(w)C'[P \mid R] \rightarrow C'[R']\{z/w\}$$

But $(w)C'[Q \mid R]$ can simulate this: we have, assuming $x \notin \mathrm{fn}(R)$,

$$(x)(ux\,.\,\{x = z\} \mid R) \rightarrow (\{x = z\})\{w/x\} \mid R'$$

and thus,

$$(w)C'[Q \mid R] \equiv (w)C'[(x)(ux\,.\,\{x = z\} \mid R)] \rightarrow (w)C'[\{z = w\} \mid R'] \rightarrow C'[R']\{z/w\}$$

i.e., $(w)C'[Q \mid R] \rightarrow^* C'[R']\{z/w\}$. So any reduction derived in this way from $C[P]$ can be simulated by $C[Q]$. It follows that $P \approx_b Q$.

A similar example without the summation operator (also by Fu) is:

$$!\,(x)ux\,.\,\{x=z\} \;\begin{array}{c}\approx_b\\ \not\approx\end{array}\; uz \mid !\,(x)ux\,.\,\{x=z\}$$

We believe that redefining the observability predicate will not improve the situation. For example, let us define an extended version of the observability predicate $\downarrow$ such that

$$P\downarrow\gamma \text{ iff } P \xrightarrow{\gamma} P' \text{ for some } P' \text{ and some communication action } \gamma$$

and let *extended* barbed congruence etc. be defined as barbed congruence with the extended predicate in place of $\downarrow$. The examples above are then not weakly extended barbed bisimilar because their extended observations do not match. However, extended barbed congruence is still different from weak hyperequivalence. An example is:

$$(x)ux\,.\,\{x=z\}\,.\,v + uz\,.\,\mathbf{0} \;\begin{array}{c}\approx_b\\ \not\approx\end{array}\; (x)ux\,.\,\{x=z\}\,.\,v + uz\,.\,\mathbf{0} + uz\,.\,v$$

These agents are extended weak barbed congruent, but are not weakly hyperequivalent.

1.2 A subcalculus

We give a semantic condition on the subclass of agents for which Lemma 4.20 (and thus Theorem 4.19) is valid. We first define an agent P to be *safe* wrt. a set of names N if $\forall P'$ s.t. $P \xrightarrow{\gamma} P'$ for some γ, if γ is a fusion then $\mathrm{n}(\gamma)\cap N=\emptyset$ and P' is safe wrt. N, and if γ is a communication action then P' is safe wrt $\mathrm{bn}(\gamma)$. We say that P is *safe* if it is safe wrt. $\emptyset$.

Although the class of safe agents is a subclass of the fusion calculus agents, it is not irrelevant. We can, e.g., see that the agents used in the encoding of the λ-calculus in Chapter 6 are indeed safe: these agents are in the f_π subcalculus with the addition of the delayed input construction $u(\tilde{x})\colon P$. Since there are no free input prefixes with objects in $\tilde{x}$ possible in P (because of syntactic restrictions), no "unsafe" fusion actions are possible.

Lemma 4.20$'$ *If P and Q are safe, then $P \approx_b Q$ implies $P \mathrel{\dot\approx} Q$.*
PROOF: We construct a family of contexts $C^{\tilde{z}}_{n,k}[\cdot]$ such that

$$\mathcal{R} = \{(P,Q) : C^{\tilde{z}}_{n,k}[P] \mathrel{\dot\approx_b} C^{\tilde{z}}_{n,k}[Q], \mathrm{fn}(P,Q)\subseteq \tilde{z}, n=|\tilde{z}|, k=\mathrm{am}(P,Q)\}$$

is a weak bisimulation, where $\mathrm{am}(P,Q)$ is the maximal arity of communication actions in P and Q.

In the definition below we postulate for each name u a fresh name u'; for each finite sequence of names $\tilde{y}$ a fresh name y''; for each finite equivalence relation e on names a fresh name m_e; an for each equivalence e and inequivalence d on pairs of names fresh names m^i_e and m^i_d for $i\geq 0$. Furthermore, $\{c, s, in, out, d_n : n\geq 0\}$ contains fresh names. Freshness guarantees that fresh names can never be confused with names used in P or Q. M_e is a sequence of match and mismatch operators agreeing with the equivalence relation e, and $\mathrm{eq}(\tilde{z})$ stands for the set of equivalence relations on names in $\tilde{z}$.

$$
\begin{array}{rcl}
C^{\tilde z}_{n,k}[\cdot] & \equiv & (\tilde z)(\cdot \mid V^k_n(\tilde z) \mid \mathit{Count}_n) \\
\mathit{Count}_n & \stackrel{def}{=} & d_n + c \,.\, \mathit{Count}_{n+1} \\
V^k_n(\tilde z) & \stackrel{def}{=} & \sum\limits_{u\in\tilde z, |\tilde y|\le k} (\tilde y) u\, \tilde y \,.\, \overline{c} \,.\, (\mathbf{1} \,.\, (u' + \mathit{out} + y'' + X(\tilde y, \tilde z\tilde y)) + \mathbf{1} \,.\, V^k_{n+|\tilde y|}(\tilde z\tilde y)) \\
 & & + \sum\limits_{u\in\tilde z, |\tilde y|\le k} (\tilde y) \overline{u}\, \tilde y \,.\, \overline{c} \,.\, (\mathbf{1} \,.\, (u' + \mathit{in} + y'' + X(\tilde y, \tilde z\tilde y)) + \mathbf{1} \,.\, V^k_{n+|\tilde y|}(\tilde z\tilde y)) \\
 & & + \ \mathbf{1} \,.\, s \\
 & & + \ \mathbf{1} \,.\, \sum\limits_{e\in \mathrm{eq}(\tilde z)} M_e m_e
\end{array}
$$

where $X(\tilde y, \tilde z\tilde y)$ stands for $\sum\limits_{i=1}^{|\tilde y|} \sum\limits_{z\in\tilde z\tilde y} ([y_i = z] m^i_{y_i=z} + [y_i \neq z] m^i_{y_i\neq z})$.

Count_n, for $n \geq 0$, is used to control the number of interactions between V and the agent put in the context: for each interaction, the observation d_n is replaced by d_{n+1}.

Note that the summations on the first two lines of the definition of V are finite up to alpha-conversion. The observables m^i_e, m^i_d in $X(\tilde y, \tilde z\tilde y)$ tell what elements of $\tilde y$ are equal to what elements of $\tilde z$ and $\tilde y$, by making a name observable corresponding to the resulting (in)equivalences for each element of $\tilde y$. Note that the position of each y_i in $\tilde y$ must be encoded in the observable name since after a fusion, $\tilde y$ needs not be pairwise distinct.

Now, for $(P, Q) \in \mathcal{R}$,

1. If $P \xrightarrow{(\tilde x)u\tilde w} P'$, we must find a Q' such that $Q \xRightarrow{(\tilde x)u\tilde w} Q'$ and $(P', Q') \in \mathcal{R}$. $C^{\tilde z}_{n,k}[P] \to\to (\tilde z)(\tilde x)(P' \mid W \mid \mathit{Count}_{n+1}) \equiv S$ where $W \equiv (\tilde x)(\mathbf{1} \,.\, (u' + \mathit{in} + y'' + X(\tilde w, \tilde z\tilde w)) + \mathbf{1} \,.\, V^k_{n+|\tilde w|}(\tilde z\tilde w))$. Now, $S \downarrow d_{n+1}$, so for $C[Q]$ to simulate the reduction, it must reduce involving Q and V. It cannot let Q communicate more than once, since $S \to S'$ s.t. $S' \downarrow d_{n+1}$ and $S' \downarrow u'$, but not $S' \to^*\downarrow d_{n+2}$. Furthermore, $S' \downarrow u'$ and $S' \downarrow \mathit{in}$, so it must be that $Q \xRightarrow{\alpha} Q'$ with $\mathrm{subj}(\alpha) = u$, and $S' \downarrow y''$, so $|\mathrm{obj}(\alpha)| = |\tilde w|$. Also, the set of observables from the $X(\tilde y, \tilde z\tilde y)$ term must be preserved. Since Q is safe, no intervening fusion can occur which affects the objects of α, so this gives $\mathrm{obj}(\alpha) = \tilde w$, where $\tilde x \subseteq \tilde w$ is fresh. Then $Q \xRightarrow{(\tilde x)u\tilde w} Q'$ and $C[Q] \to^* (\tilde z)(\tilde x)(Q' \mid W \mid \mathit{Count}_{n+1}) \equiv T$. Finally the reduction $S \to C^{\tilde z\tilde w}_{n+|\tilde w|,k}[P']$ must be simulated by $T \to C^{\tilde z\tilde w}_{n+|\tilde w|,k}[Q']$ since $C^{\tilde z\tilde w}_{n+|\tilde w|,k}[P'] \to S''$ s.t. $S'' \downarrow s$ and $S'' \downarrow d_{n+1}$, but not $S'' \to^*\downarrow d_{n+2}$.

2. If $P \xrightarrow{(\tilde x)\overline{u}\,\tilde w} P'$ the argument is symmetric.

3. If $P \xrightarrow{\varphi} P'$, then $C^{\tilde z}_{n,k}[P] \to C^{\tilde z}_{n,k}[P']\sigma \to S'''$ s.t. $S''' \downarrow m_e$ and $S''' \downarrow d_n$ for σ agreeing with φ and m_e encoding the equivalence relation of names in $\tilde z$ agreeing with φ. To preserve this observation, it must be that $Q \xRightarrow{\varphi} Q'$, i.e., Q can perform a sequence of fusion actions which "sum up" to the same effect as φ. There can be no interaction between Q and V since not $S''' \to^*\downarrow d_{n+1}$. Then $C^{\tilde z}_{n,k}[Q] \xRightarrow{\mathbf{1}} C^{\tilde z}_{n,k}[Q']\sigma \downarrow m_e$; if $Q \xRightarrow{\psi} Q'$ for some ψ different from φ, $m_f \neq m_e$ will be observable.

Thus, the relation $\mathcal{R}$ is a weak bisimulation. □

Theorem 4.19′ *$P \approx Q$ implies $P \approx_b Q$. If P and Q are safe, then $P \approx_b Q$ implies $P \approx Q$.*
PROOF: Every weak hyperbisimulation is clearly a weak barbed bisimulation, so $\approx \subseteq \dot\approx_b$, and since $\approx$ is a congruence the also $\approx \subseteq \approx_b$. If P and Q are safe, then by Theorem 4.9 and Lemma 4.20′ $P \approx_b Q$ implies $P \approx Q$. □

1.3 Strong barbed congruence

To avoid any uncertainty as to the validity of the strong case, we also show how the proof of Lemma 4.18 differs from that of Lemma 4.20′.

Lemma 4.18 *Barbed congruence is contained in bisimulation.*
PROOF: We construct a family of contexts $C^{\tilde{z}}_{n,k}[\cdot]$ such that

$$\mathcal{R} = \{(P,Q) : C^{\tilde{z}}_{n,k}[P] \mathrel{\dot\sim_b} C^{\tilde{z}}_{n,k}[Q], \mathrm{fn}(P,Q) \subseteq \tilde{z}, n = |\tilde{z}|, k = \mathrm{am}(P,Q)\}$$

is a bisimulation, where $\mathrm{am}(P,Q)$ is the maximal arity of communication actions in P and Q. The context used is simpler because we have control over the number of reductions made by the simulating agent.

$$\begin{array}{rcl} C^{\tilde{z}}_{n,k}[\cdot] & \equiv & (\tilde{z})(\cdot \mid V^k_n(\tilde{z})) \\ V^k_n(\tilde{z}) & \stackrel{def}{=} & \sum\limits_{u\in\tilde{z},|\tilde{y}|\le k} (\tilde{y})u\,\tilde{y}\,.\,(u' + out + y'' + X(\tilde{y},\tilde{z}\tilde{y}) + \mathbf{1}\,.\,V^k_{n+|\tilde{y}|}(\tilde{z}\tilde{y})) \\ & & +\ \sum\limits_{u\in\tilde{z},|\tilde{y}|\le k} (\tilde{y})\overline{u}\,\tilde{y}\,.\,(u' + in + y'' + X(\tilde{y},\tilde{z}\tilde{y}) + \mathbf{1}\,.\,V^k_{n+|\tilde{y}|}(\tilde{z}\tilde{y})) \\ & & +\ s \\ & & +\ \mathbf{1}\,.\sum\limits_{e\in\mathrm{eq}(\tilde{z})} M_e m_e \end{array}$$

where $X(\tilde{y},\tilde{z}\tilde{y})$ stands for $\sum\limits_{i=1}^{|\tilde{y}|}\sum\limits_{z\in\tilde{z}\tilde{y}}([y_i = z]m^i_{y_i=z} + [y_i \neq z]m^i_{y_i\neq z})$.

Now, for $(P,Q) \in \mathcal{R}$,

1. If $P \xrightarrow{(\tilde{x})u\tilde{w}} P'$, we must find a Q' such that $Q \xrightarrow{(\tilde{x})u\tilde{w}} Q'$ and $(P',Q') \in \mathcal{R}$. This is done in a similar way to the proof of Lemma 4.20′, but simpler.

2. If $P \xrightarrow{(\tilde{x})\overline{u}\,\tilde{w}} P'$ the argument is symmetric.

3. If $P \xrightarrow{\varphi} P'$, then we handle this just like for the weak case, but with a single simulating reduction and a single simulating transition.

Thus, the relation $\mathcal{R}$ is a bisimulation. □

1.4 Impact

We have demonstrated that Theorem 4.19 is false as stated in that weak hyperequivalence is strictly stronger than weak barbed congruence. This has no impact on other results in the thesis (Theorem 4.19 is never used). In Section 6.2 of the thesis weak barbed bisimulation can safely be substituted by weak hyperequivalence, since both ignore divergence, and this property is sufficient there.

Admittedly this detracts somewhat from the motivation behind weak hyperequivalence, which perhaps is not as canonical as we first thought. We maintain that weak hyperequivalence still has ample motivation in the convenient coinductive definition, making the results on axiomatizations and algorithms interesting. A similar coinductive definition of weak barbed congruence is high on the agenda for future work.

2 Minor errors

Page	Line	Reads	Should be
14	12	$\xrightarrow{\mathbf{1}}$ (twice)	$\xrightarrow{\tau}$ (twice)
15	-10		append "where **1** is the identity relation"
17	2	equivalence.	equivalence [MS92a,San93].
25	15	relate	related
26	13		append "$, n \geq 0$"
28	-12	$(\boldsymbol{\nu})$	$(\boldsymbol{\nu} u)$
31	1		erase "$\tilde{M}_1$"
31	2		erase "$\tilde{M}_1 \Leftrightarrow$"
31	5		erase "$\tilde{M}$"
40	14	n(init(R, R'))	init(R, R')
40	-4	$\{r_y, \overline{r_y}\}$	$\{r_y\}$
93	5		append "Here and in the following we write $\overline{u}\langle x, \boldsymbol{\nu} y, z\rangle . P$ for $(\boldsymbol{\nu} y)\overline{u}\langle x, y, z\rangle . P$, and we use an underscore _ to signify a name not used anywhere else."
97	24	we give	We give
98	-7		erase "what"
113	-3	strengthens	weakens