Solving a Control Problem

Tom Verhoeff

Department of Mathematics and Computing Science
Eindhoven University of Technology
P.O. Box 513
NL–5600 MB EINDHOVEN
The Netherlands
wstomv@win.tue.nl

September 1990
Revised January 1991

0 Introduction

In Trace Theory, the communication behavior of a mechanism is specified by means of a *trace structure*. Parallel composition of such mechanisms is modeled by the *weaving* operator **w** and hiding of actions (making them internal) is modeled by the *projection* operator $\upharpoonright$. Parallel composition followed by internalization of the communication channels between two mechanisms is modeled by the *blending* operator **b**. It is a combination of weaving and projection on the external channels. The refinement order, expressing when one mechanism is at least as good as another, is modeled by the *inclusion* relation $\subseteq$.

In his dissertation [3], Smedinga studies the following *control problem* (see p. 29). Given trace structures P, $L_{\min}$, and $L_{\max}$, find trace structure R such that

$$L_{\min} \subseteq P \,\mathbf{b}\, R \subseteq L_{\max}. \qquad (0)$$

$L_{\min}$ and $L_{\max}$ delineate a desired behavior for a mechanism that is to be implemented as the composition of a known mechanism P with some yet unknown controller R. When $L_{\min} = L_{\max} = L$, we obtain the *reduced control problem* of finding R such that

$$P \,\mathbf{b}\, R = L. \qquad (1)$$

In this note, we present a solution to the control problem. We also briefly look into the case that the trace structures are all required to be non-empty and prefix-closed. We compare our solution to that of Smedinga. Finally, we argue that Smedinga's interpretation of an arbitrary trace structure as a specification for the communication behavior of a mechanism is not in agreement with the intended interpretation of the weaving and projection operators and that a better approach might be to use the failures model of CSP [0]. This would also take care of deadlock issues.

Acknowledgement

This note was inspired by a discussion with Jacko Koster who did some research on the control problem for his Master's thesis (*Een methode voor het oplossen van besturingsproblemen in tracetheorie*, August 1990).

1 Preliminary Theory

In this section, we briefly summarize the relevant parts of Trace Theory. For more details, the reader is referred to [2].

A trace structure is a pair $\langle A, S\rangle$ where A is a set of symbols and S is a set of traces over A, that is, $S \subseteq A^*$. A is called the *alphabet* and S the *trace set* of the trace structure. For the time being we ignore the issue of interpreting a trace structure as specifying the communication behavior of a mechanism. Selector functions $\mathbf{a}$ and $\mathbf{t}$ on trace structures are defined by

$$T \quad = \quad \langle \mathbf{a}T, \mathbf{t}T\rangle.$$

Trace structure $STOP$ is defined by

$$STOP \quad = \quad \langle \varnothing, \{\varepsilon\}\rangle,$$

where ε is the empty trace (of length zero). *Inclusion* relation $\subseteq$ on trace structures is defined by

$$T \subseteq U \quad \equiv \quad \mathbf{a}T = \mathbf{a}U \ \wedge \ \mathbf{t}T \subseteq \mathbf{t}U.$$

Weaving operator $\mathbf{w}$ on trace structures is defined by

$$T \,\mathbf{w}\, U \quad = \quad \langle \mathbf{a}T \cup \mathbf{a}U, \{t \in (\mathbf{a}T \cup \mathbf{a}U)^* \mid t{\restriction}\mathbf{a}T \in \mathbf{t}T \ \wedge \ t{\restriction}\mathbf{a}U \in \mathbf{t}U\}\rangle,$$

where $t{\restriction}A$ is the *projection* of trace t on alphabet A, that is, the trace obtained by removing from t all symbols not in A. For alphabet A, *projection* operator ${\restriction}A$ on trace structures is defined by

$$T{\restriction}A \quad = \quad \langle \mathbf{a}T \cap A, \{t{\restriction}A \mid t \in \mathbf{t}T\}\rangle.$$

Blending operator $\mathbf{b}$ on trace structures is now defined by

$$T \,\mathbf{b}\, U \quad = \quad (T \,\mathbf{w}\, U){\restriction}(\mathbf{a}T \div \mathbf{a}U).$$

Weaving and blending are commutative and $\subseteq$-monotonic, and have $STOP$ as unit. Weaving is associative in general and, if each symbol occurs in at most two of the alphabets of the trace structures involved, then blending is also associative. Furthermore, we have

$$T \,\mathbf{b}\, U = \langle \varnothing, \varnothing\rangle \quad \equiv \quad \mathbf{a}T = \mathbf{a}U \ \wedge \ \mathbf{t}T \cap \mathbf{t}U = \varnothing. \tag{2}$$

Proof We derive

$$\begin{array}{ll}
& T \,\mathbf{b}\, U = \langle \varnothing, \varnothing\rangle \\
\equiv & \quad \{ \text{ definition of } \mathbf{b} \ \} \\
& \mathbf{a}T \div \mathbf{a}U = \varnothing \ \wedge \ \mathbf{t}(T \,\mathbf{w}\, U){\restriction}(\mathbf{a}T \div \mathbf{a}U) = \varnothing \\
\equiv & \quad \{ \text{ set theory, property of } {\restriction}\text{: } \mathbf{t}T{\restriction}A = \varnothing \equiv \mathbf{t}T = \varnothing \ \} \\
& \mathbf{a}T = \mathbf{a}U \ \wedge \ \mathbf{t}(T \,\mathbf{w}\, U) = \varnothing \\
\equiv & \quad \{ \text{ property of } \mathbf{w}\text{: } \mathbf{a}T = \mathbf{a}U \Rightarrow \mathbf{t}(T \,\mathbf{w}\, U) = \mathbf{t}T \cap \mathbf{t}U \ \} \\
& \mathbf{a}T = \mathbf{a}U \ \wedge \ T \cap U = \varnothing
\end{array}$$

∎

Reflection operator

We now define a new unary operator on trace structures, called *reflection* and denoted by $\backsim$. It is defined by

$$\backsim T \quad = \quad \langle \mathbf{a}T, (\mathbf{a}T)^* \setminus \mathbf{t}T \rangle.$$

It satisfies a number of interesting and useful properties. For instance, reflection reverses the inclusion order:

$$T \subseteq U \quad \equiv \quad \backsim U \subseteq \backsim T. \tag{3}$$

Reflection is its own inverse:

$$\backsim\backsim T \quad = \quad T. \tag{4}$$

Reflecting $STOP$, the unit of weaving and blending, yields the empty trace structure:

$$\backsim STOP \quad = \quad \langle \varnothing, \varnothing \rangle.$$

The following property expresses a fundamental relationship between the inclusion order, reflection, and blending:

$$T \subseteq U \quad \equiv \quad T \,\mathbf{b}\, \backsim U = \langle \varnothing, \varnothing \rangle. \tag{5}$$

Proof We derive

$$
\begin{array}{ll}
& T \subseteq U \\
\equiv & \quad \{ \text{ definition of } \subseteq \} \\
& \mathbf{a}T = \mathbf{a}U \ \wedge \ \mathbf{t}T \subseteq \mathbf{t}U \\
\equiv & \quad \{ \text{ set theory } \} \\
& \mathbf{a}T = \mathbf{a}U \ \wedge \ \mathbf{t}T \cap ((\mathbf{a}U)^* \setminus \mathbf{t}U) = \varnothing \\
\equiv & \quad \{ \text{ definition of } \backsim \} \\
& \mathbf{a}T = \mathbf{a}(\backsim U) \ \wedge \ \mathbf{t}T \cap \mathbf{t}(\backsim U) = \varnothing \\
\equiv & \quad \{ \ (2) \ \} \\
& T \,\mathbf{b}\, \backsim U = \langle \varnothing, \varnothing \rangle
\end{array}
$$

■

Finally, we arrive at the most important property, which can be interpreted as a *factorization formula*:

$$T \,\mathbf{b}\, U \subseteq V \quad \equiv \quad T \subseteq \backsim(U \,\mathbf{b}\, \backsim V). \tag{6}$$

Proof We derive

$$
\begin{array}{ll}
& T \,\mathbf{b}\, U \subseteq V \\
\equiv & \quad \{ \ (5), \text{ definition of } \mathbf{b} \ \} \\
& (T \,\mathbf{b}\, U) \,\mathbf{b}\, \backsim V = \langle \varnothing, \varnothing \rangle \ \wedge \ \mathbf{a}T \div \mathbf{a}U = \mathbf{a}V \\
\equiv & \quad \{ \ \mathbf{b} \text{ associative because } \mathbf{a}T \cap \mathbf{a}U \cap \mathbf{a}(\backsim V) = \varnothing \ \} \\
& T \,\mathbf{b} (U \,\mathbf{b}\, \backsim V) = \langle \varnothing, \varnothing \rangle \ \wedge \ \mathbf{a}T \div \mathbf{a}U = \mathbf{a}V \\
\equiv & \quad \{ \ (4), \text{ set theory } \} \\
& T \,\mathbf{b}\, \backsim\backsim(U \,\mathbf{b}\, \backsim V) = \langle \varnothing, \varnothing \rangle \ \wedge \ \mathbf{a}T = \mathbf{a}U \div \mathbf{a}V \\
\equiv & \quad \{ \ (5), \text{ definition of } \mathbf{b} \ \} \\
& T \subseteq \backsim(U \,\mathbf{b}\, \backsim V)
\end{array}
$$

■

2 Solutions to the Control Problem

We now consider the control problem (0) again. We claim that it has a solution if and only if

$$L_{\min} \subseteq P\,\mathbf{b}\backsim(P\,\mathbf{b}\backsim L_{\max}). \tag{7}$$

Furthermore, if it is solvable then $\backsim(P\,\mathbf{b}\backsim L_{\max})$ is the $\subseteq$-greatest solution.

Proof We derive (7) as solvability condition:

$$\begin{array}{ll} & (\exists\, R :: L_{\min} \subseteq P\,\mathbf{b}\,R \subseteq L_{\max}) \\ \equiv & \quad \{\ (6),\text{ using commutativity of } \mathbf{b}\ \} \\ & (\exists\, R :: L_{\min} \subseteq P\,\mathbf{b}\,R \ \wedge\ R \subseteq \backsim(P\,\mathbf{b}\backsim L_{\max})) \\ \equiv & \quad \{\ \Rightarrow:\ \mathbf{b}\text{ is } \subseteq\text{-monotonic; } \Leftarrow:\text{ take } R := \backsim(P\,\mathbf{b}\backsim L_{\max})\ \} \\ & L_{\min} \subseteq P\,\mathbf{b}\backsim(P\,\mathbf{b}\backsim L_{\max}) \end{array}$$

The greatest solution—if there exists one—is now also obvious. ■

The solvability condition can be effectively computed for *regular* (i.e., finite state) trace structures, because all operators involved, including reflection, are effectively computable, for example, in terms of *state graphs.*

In Trace Theory, only non-empty prefix-closed trace structures, i.e., T such that

$$\mathbf{t}T \neq \varnothing \quad \wedge \quad (\forall\, s,t : st \in \mathbf{t}T : s \in \mathbf{t}T),$$

are used to specify the communication behavior of mechanisms. These trace structures are called *processes.*

For processes P and L, in general, $\backsim(P\,\mathbf{b}\backsim L)$ need not be a process. Consider, for example,

$$\begin{array}{lcl} L &=& \langle\{a\},\{\varepsilon\}\rangle, \\ P &=& \langle\{a,x\},\{\varepsilon,a\}\rangle. \end{array}$$

Then we have

$$\begin{array}{rcl} \backsim L &=& \langle\{a\},\{a^n \mid n \geqslant 1\}\rangle, \\ P\,\mathbf{b}\backsim L &=& \langle\{x\},\{a{\restriction}\{x\}\}\rangle \ = \ \langle\{x\},\{\varepsilon\}\rangle, \\ \backsim(P\,\mathbf{b}\backsim L) &=& \langle\{x\},\{x^n \mid n \geqslant 1\}\rangle. \end{array}$$

The latter is not prefix-closed. In this case, because it does not contain ε, there is no solution to the reduced control problem (1) for P and L in terms of processes.

The *prefix-interior* of trace structure T, denoted T°, is defined by

$$T^\circ \quad = \quad \langle \mathbf{a}T, \{t \in \mathbf{t}T \mid (\forall\, s : s \leqslant t : s \in \mathbf{t}T)\}\rangle,$$

where $s \leqslant t$ expresses that s is a prefix of t. T° is the $\subseteq$-greatest prefix-closed trace structure contained in T. It is effectively computable for regular trace structures. We now obviously have that the control problem (0) is solvable for prefix-closed—but possibly empty— R if and only if

$$L_{\min} \quad \subseteq \quad P\,\mathbf{b}\,T,$$

where $T = (\backsim(P\,\mathbf{b}\backsim L_{\max}))^\circ$. Furthermore, T is the $\subseteq$-greatest prefix-closed solution, if one exists. If T is empty, i.e., $\mathbf{t}T = \varnothing$, then the control problem is not solvable for processes R.

Smedinga's solution method

Smedinga solves a restricted version of the control problem in [3, Ch. 3], viz. by considering only trace structures P and L such that $\mathbf{a}L \subseteq \mathbf{a}P$ and R such that $R \subseteq P{\upharpoonright}(\mathbf{a}P \setminus \mathbf{a}L)$. Furthermore, he expresses the solutions in terms of, what one might call, a *relativized* reflection operator (see pp. 32 and 35):

$$R_{\max} \quad = \quad (P\,\mathbf{b}\,L_{\max}) \setminus (P\,\mathbf{b}((P{\upharpoonright}\mathbf{a}L_{\max}) \setminus L_{\max})),$$

where for trace structures T and U with $\mathbf{a}T = \mathbf{a}U$ we define the trace structure $T \setminus U$, called the reflection of T relative to U, by

$$T \setminus U \quad = \quad \langle \mathbf{a}T, \mathbf{t}T \setminus \mathbf{t}U \rangle.$$

Note that our reflection operator can be expressed in terms of relativized reflection by

$$\backsim T \quad = \quad \langle \mathbf{a}T, (\mathbf{a}T)^* \rangle \setminus T.$$

Our reflection operator is algebraically much nicer to deal with than Smedinga's relativized reflection and it allows a straightforward treatment of the general control problem.

Deadlock

There is still the problem that solutions to the control problem may not be acceptable after all, because of *deadlock*. We have not looked into this carefully, but employing the failures model, as we will suggest in the next section, should also take care of this.

3 Interpretation of Trace Structures as Specifications

In Trace Theory, process T, i.e., a non-empty prefix-closed trace structure, is interpreted as specification for the communication behavior of a mechanism in one of the following two ways. Under both interpretations, the alphabet of T determines the set of communication ports of the mechanism, through which interaction with the environment takes place. Furthermore, the trace set of T consists of all *possible* communication histories.

In the first interpretation, this means that if $ta \in \mathbf{t}T$ (and, hence, also $t \in \mathbf{t}T$) then the process *may* (but need not) engage in a communication along channel a after t has taken place. Actual occurrence of a after t may depend both on the environment and the "internal" state of the process after t. On the other hand, if $t \in \mathbf{t}T$ and $ta \notin \mathbf{t}T$, then communication along a is blocked unconditionally after t. This is a very weak interpretation (as far as progress is concerned), but the intended meaning of weaving and projection agrees with it.

In the second interpretation, if $ta \in \mathbf{t}T$ then the process is required to perform *some* successor action b after t such that $tb \in \mathbf{t}T$, but not necessarily $b = a$ (the actual choice of successor may depend on the environment and the "internal" state of the process). Again, if $t \in \mathbf{t}T$ and $ta \notin \mathbf{t}T$ then communication along a after t is unconditionally blocked. Only if $t \in \mathbf{t}T$ and for no $a \in \mathbf{a}T$ do we have $ta \in \mathbf{t}T$, is the process allowed to *terminate*. This is a strong interpretation (as far as progress is concerned). For weaving we now have to consider the possibility of deadlock, where a process has a progress obligation which it cannot meet because it is curtailed by its environment. This is not captured directly by the weaving operator. Similarly, projection does not faithfully preserve this interpretation. In [2], the notions of *lock* and *transparency* were introduced to handle these problems. Also, the inclusion relation no longer expresses refinement and it is not possible to express all kinds of non-determinism.

A more general model that treats deadlock and non-determinism is the *failures model* for CSP [0]. However, it does not admit a reflection operator, unless the domain of processes is extended. How this extension should be done is a subject for future research.

Smedinga's interpretation

Smedinga's interpretation of an *arbitrary* trace structure T as specifying the communication behavior of a mechanism is as follows (cf. [3, p. 24]). The alphabet determines the set of communication ports (same as above) and the trace set determines the set of *completed tasks*, i.e., communication histories after which the process may become *quiescent* (fail to continue). Hence, trace set inclusion indeed expresses refinement. The trace structure with an empty trace set, plays the role of a *miracle* because it has no failures (does not become quiescent) and nevertheless engages in no communications. It refines every trace structure. For these reasons it is excluded in [3].

Smedinga's interpretation is problematic, at least when dealing with synchronous (rendezvous type) interaction. (For a consistent interpretation along these lines in an asynchronous setting see [1].) For instance, the weaving operator suffers from the following deficiency. Consider trace structures T and U defined by

$$\begin{aligned} T &= \langle \{a, b\}, \{(ab)^n \mid n \geqslant 0\}\rangle, \\ U &= \langle \{a, b\}, \{a(ba)^n \mid n \geqslant 0\}\rangle. \end{aligned}$$

Because all traces in T are of even length and all traces in U are of odd length, we then have

$$T \,\mathbf{w}\, U \quad = \quad \langle \{a, b\}, \varnothing\rangle.$$

However, we would expect the parallel composition to yield a trace structure that describes a mechanism alternately engaging in a and b actions (starting with a) and never becoming quiescent. This deficiency can be overcome by allowing infinite traces in the trace sets. Both $\mathbf{t}T$ and $\mathbf{t}U$ could be extended with $(ab)^\omega$, in which case their weave would also contain this trace and thus be non-empty as expected.

The projection operator is also problematic as the following example shows. Consider trace structure T defined by

$$T \quad = \quad \langle \{a, b, x, y\}, \{ax, by\}\rangle.$$

Then we have

$$T \upharpoonright \{x, y\} \quad = \quad \langle \{x, y\}, \{x, y\}\rangle,$$

but from an operational point of view the trace ε is "partially" quiescent in the projected trace structure, because T could (internally) choose to do b, thereby blocking communication along x. Consider as environment the trace structure U defined by

$$U \quad = \quad \langle \{x, y\}, \{x\}\rangle.$$

Then we would have

$$T \,\mathbf{w}\, U \quad = \quad \langle \{a, b, x, y\}, \{ax\}\rangle,$$

which expresses that initial action b is to be blocked and this implies backtracking if action b is actually internal to T. To capture "partial" quiescence precisely, something along the lines of refusal sets as in the failures model are required, or one should consider asynchronous instead of synchronous interaction.

Implications

In my opinion, the control problem should be expressed as: Given P and L find R such that

$$P \,\mathbf{b}\, R \subseteq L. \tag{8}$$

The additional requirement imposed by (0), viz. $L_{\min} \subseteq P \,\mathbf{b}\, R$, is a no more than clumsy way to exclude some solutions that—although correct under the weak interpretation—are not desirable under a stronger interpretation. "Bare" trace structures, however, are not a suitable model for these stronger interpretations anyway. Using an extended model—for example, the failures model or the receptive processes model—will overcome this problem and will give rise to a formulation similar in form to (8).

4 Conclusion

In this note, we have formulated a control problem using the terminology of Trace Theory. An elegant solution to this control problem has been presented with the aid of a newly defined reflection operator. Finally, we have analyzed some interpretations of trace structures as specifications and we have criticized the formulation of the control problem. This has lead us to suggest further research on the analogous control problem in the failures model of CSP and the receptive processes model, which requires a suitable extension of the process domains involved.

References

[0] C. A. R. Hoare. *Communicating Sequential Processes.* Prentice-Hall, 1985.

[1] M. B. Josephs. Receptive process theory. Computing Science Notes 90/8, Dept. of Math. and C.S., Eindhoven Univ. of Technology, Sept. 1990.

[2] A. Kaldewaij. *A Formalism for Concurrent Processes.* PhD thesis, Dept. of Math. and C.S., Eindhoven Univ. of Technology, 1986.

[3] R. Smedinga. *Control of Discrete Events.* PhD thesis, Rijksuniversiteit Groningen, The Netherlands, 1989.