Universität Augsburg

Tracelets and Specifications

T. Hoare, B. Möller, M. E. Müller

Report 2017-01 January 2017

Institut für Informatik
D-86135 Augsburg

Tracelets and Specifications

T. Hoare[1], B. Möller[2], and M. E. Müller[3]

[1] Microsoft Research, Cambridge, UK
[2] Institut für Informatik, Universität Augsburg, Germany
[3] Fachbereich Informatik, Hochschule Bonn-Rhein-Sieg, Germany

Abstract. In the accompanying paper [1] the authors study a model of concurrent programs in terms of events and a dependence relation, i.e., a set of *arrows*, between them. There also two simplifying *interface models* are presented; they abstract in different ways from the intricate network of internal points and arrows of program components. This report supplements [1] by presenting full proofs for the properties of the interface models, in particular, that both models exhibit homomorphic behaviour w.r.t. sequential and concurrent composition.

Keywords: Concurrent Kleene Algebra, Laws of Programming, Trace Algebra, Semantic Models, Refinement, Unifying Theories

1 Introduction

In [1] the authors present a model of concurrent programs in terms of events (more abstractly called *points*) and a dependence relation, i.e., a set of *arrows*, between them. A subset of points and the corresponding arrows them form a *tracelet*. Sect. 6 of [1] gives a simpler (more abstract) model. It abstracts from the intricate network of internal points and arrows of a tracelet, and defines sequential and concurrent composition solely in terms of the interface arrows between the operands. The common part of their interfaces is removed, and the rest forms the interface of the result of the composition. For some purposes, this interface model is an oversimplification, because it fails to model the phenomenon of deadlock resulting from a cyclic chain of causation. Cyclicity is a programming error that halts a group of threads, when each of them is waiting for occurrence of actions of other members of the cycle. This problem is solved by a second model, which retains the internal causal connectivity between the arrows of the perimeter. This model enables absence of deadlock to be proved, or at least detected.

This report supplements [1] by presenting the full proofs for the properties of these two interface models, in particular, that both models exhibit homomorphic behaviour w.r.t. sequential and concurrent composition.

2 Traces and Tracelets

Let Pt be a set of *points* which may, e.g., stand for events in a program execution. A *trace* is a pair $H = (\mathsf{Pt}, \mathsf{Dep})$ where $\mathsf{Dep} \subseteq \mathsf{Pt} \times \mathsf{Pt}$ is a binary *dependence* relation representing between points; the elements of Dep are called *arrows*. A *pre-tracelet* within H is a pair $G = (E, A)$ such that $E \subseteq \mathsf{Pt}$ and $A \subseteq \mathsf{Dep}^+$, where $^+$ denotes transitive closure. The points in E are considered to be inside G, the ones in $\overline{E}$, the complement of E, outside. *Internal* arrows $(x, y) \in A$ have both points x, y in E, while *interface* arrows have one point inside and the other outside. We give algebraic definitions of the various sorts of arrows in a tracelet:

$$\begin{array}{llll} \mathit{hidar}(G) & =_{df} & A \cap E \times E \ , & (\textit{hidden} \text{ arrows}) \\ \mathit{inar}(G) & =_{df} & A \cap \overline{E} \times E \ , & (\textit{input} \text{ arrows}) \\ \mathit{outar}(G) & =_{df} & A \cap E \times \overline{E} \ . & (\textit{output} \text{ arrows}) \end{array}$$

The sets $\mathit{in}(G)$ of *input points* and $\mathit{out}(G)$ of *output points* are defined as the codomain of $\mathit{inar}(G)$ and the domain of $\mathit{outar}(G)$, resp.

A *pre-tracelet* $G = (E, A)$ is called a *tracelet* if A is the set of arrows in Dep that have at least one end point in E. This healthiness condition is formalised as

$$A \ = \ \mathsf{Dep} \cap (E \times \mathsf{Pt} \cup \mathsf{Pt} \times E) \ . \qquad \text{(saturation)} \qquad (1)$$

It entails that A must not contain "loose" arrows that "bypass" the points of A:

$$A \cap \overline{E} \times \overline{E} \ = \ \emptyset \ . \qquad \text{(no loose arrows)} \qquad (2)$$

All proofs are deferred to Sect. 5.

3 The Simple Specification of a Tracelet

A specification of a tracelet G is a pre-tracelet that eliminates all details of internal value propagation in G. In this section we deal with *simple specifications* that only record input and output from/to the environment. A more refined version will be discussed in the next section.

Formally we set

$$\mathit{sspec}(G) \ =_{df} \ (\mathit{in}(G) \cup \mathit{out}(G), \mathit{inar}(G) \cup \mathit{outar}(G)) \ .$$

Theorem 3.1

1. *$\mathit{inar}(\mathit{sspec}(G)) = \mathit{inar}(G)$ and $\mathit{outar}(\mathit{sspec}(G)) = \mathit{outar}(G)$.*
2. *Consequently, $\mathit{in}(\mathit{sspec}(G)) = \mathit{in}(G)$ and $\mathit{out}(\mathit{sspec}(G)) = \mathit{out}(G)$. Moreover, $\mathit{hidar}(\mathit{sspec}(G)) = \emptyset$.*
3. *All this implies that sspec is idempotent: $\mathit{sspec}(\mathit{sspec}(G)) = \mathit{sspec}(G)$.*

We now show that *sspec* is a homomorphism from general tracelets to specifications w.r.t. the composition operator | from [2] that is defined as follows. For pre-tracelets G, G' with disjoint point sets,

$$G \mid G' =_{df} (E + E', A \cup A') ,$$

where + denotes disjoint union. It is clear that this is a pre-tracelet again.

Assume now that G and G' are tracelets. Using distributivity of relational composition it is straightforward to show that $G \mid G'$ is a tracelet again. Moreover, by the saturation assumption we have $\mathrm{AGR}(G, G')$, where

$$\begin{array}{rl} \mathrm{AGR}(G, G') \iff_{df} & A \cap E \times E' = A' \cap E \times E' \ \wedge \\ & A \cap E' \times E = A' \cap E' \times E \ . \end{array} \tag{3}$$

An equivalent formulation is the following.

Lemma 3.2
$\mathrm{AGR}(G, G') \iff \forall F \subseteq E, F' \subseteq E' : F\, A\, F' = F\, A'\, F' \wedge F'\, A\, F = F'\, A'\, F.$

The goal now is to show for tracelets G, G' the homomorphic equation

$$sspec(G \mid G') = sspec(sspec(G) \mid sspec(G')) .$$

The equation is homomorphic in the following sense. One can define a new operator $|'$ on specifications G, G' by $G|'G' =_{df} sspec(G \mid G')$. Then $sspec(G \mid G') = sspec(G)|'sspec(G')$.

We need a few auxiliary properties. First we establish the behaviour of the *inar*, *outar* and *hidar* functions on composed traces.

Lemma 3.3 *Let G, G' be tracelets with $E \cap E' = \emptyset$ and set $\widetilde{G} =_{df} G \mid G'$.*

$$\begin{array}{r} inar(\widetilde{G}) = (inar(G) \cap \overline{E'} \times \mathsf{Pt}) \cup (inar(G') \cap \overline{E} \times \mathsf{Pt}) \ , \\ outar(\widetilde{G}) = (outar(G) \cap \mathsf{Pt} \times \overline{E'}) \cup (outar(G') \cap \mathsf{Pt} \times \overline{E}) \ . \end{array}$$

Moreover, $\mathrm{AGR}(G, G')$ *implies*

$$hidar(\widetilde{G}) = hidar(G) \cup hidar(G') \cup (A \cap A') .$$

Now we can say something about the behaviour of interfaces under specification and composition.

Lemma 3.4

$$\begin{array}{r} inar(sspec(G \mid G')) \subseteq inar(sspec(sspec(G) \mid sspec(G'))) \ , \\ outar(sspec(G \mid G')) \subseteq outar(sspec(sspec(G) \mid sspec(G'))) \ . \end{array}$$

This is independent of the saturation condition (1). Employing (1) yields also the reverse inclusions so that we obtain the desired result.

Theorem 3.5 *For tracelets G, G' with $E \cap E'$ we have*

$$sspec(G \mid G') = sspec(sspec(G) \mid sspec(G')) \ .$$

4 The Refined Specification of a Tracelet

The *refined specification* $spec(G)$ is a pre-tracelet that additionally records whether input and output points are connected or are separated by deadlock or the like.

To this end, every proper chain of internal arrows between an input and an output point is replaced by a single arrow. Formally:

$$spec(G) \ =_{df} \ (in(G) \cup out(G), inar(G) \cup outar(G) \cup co)$$

where $co \ =_{df} \ hidar(G)^+ \ \cap \ in(G) \times out(G)$.

This refined operator is again idempotent:

Theorem 4.1 $spec(spec(G)) = spec(G)$.

Next we show that the homomorphic property also holds for *spec*. This is done in two steps.

Lemma 4.2 *Set again $\widehat{G} \ =_{df} \ spec(G)$ etc. and define co, co' as in Sect. 4.*

1. $\widehat{A} \cap \widehat{A}' = A \cap A'$.
2. $hidar(\widehat{G} \mid \widehat{G}') = co \ \cup co' \cup (A \cap A')$.
3. $hidar(spec(\widehat{G} \mid \widehat{G}')) \subseteq hidar(spec(G \mid G'))$.

Now we show also the reverse inclusion

$$hidar(spec(\widehat{G} \mid \widehat{G}')) \subseteq hidar(spec(G \mid G')) \ ,$$

which, using the definitions and Lm. 4.2.1, spells out to

$$(hidar(G) \cup hidar(G') \cup C)^+ \ \cap \ \tilde{i} \times \tilde{o} \quad \subseteq \quad (co \ \cup co' \cup C)^+ \ \cap \ \tilde{i} \times \tilde{o} \ , \qquad (4)$$

where $\tilde{i} \ =_{df} \ in(G) \cup in(G'), \tilde{o} \ =_{df} \ out(G) \cup out(G')$ and $C \ =_{df} \ A \cap A'$. After that we are done, since every tracelet is determined by its points and its *inar*, *outar* and *hidar* sets.

Let us first give an intuitive idea why (4) holds. Consider point-disjoint tracelets G, G' and points $e \in i, e' \in o'$ such that $e\widetilde{ha}^+e'$. Consider an arbitrary path p

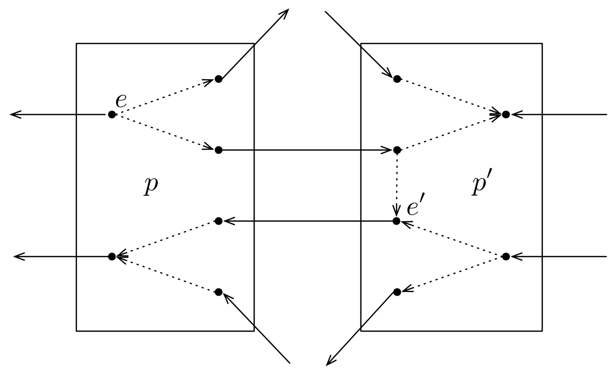

Fig. 1. Connection paths in a composition

from e to e' in $\widetilde{ha}$. According to Lm. 3.3 we can group p into maximal pieces that are purely within ha, purely within ha' or consist only of arrows in C. The reason is that arrows from ha cannot connect directly with those from ha', because their end points lie in disjoint point sets. They can only connect via "bridges" in C. Now each of the maximal pieces within ha or ha' can be contracted to a single ha^+ or ha'^+ edge, as is done by *spec*. By maximality they have to start and end in points in $i \cup o$ or $i' \cup o'$, resp., which makes their contractions belong to co or co', resp. Therefore it does not matter if we contract a composition tracelet directly or first contract its maximal pieces and then contract the result further.

The formal proof uses regular algebra to good advantage. We recall some of its standard laws, denoting relational composition by juxtaposition. For relations R, S, we have

$$R^+ = R\,R^* = R^*\,R \;, \tag{5}$$

$$R^* = I \cup R^+ \;, \tag{6}$$

$$(R \cup S)^* = R^*\,(S\,R^*)^* \;. \tag{7}$$

We have to deal with the subexpression $(hidar(G) \cup hidar(G') \cup C)^+$ occurring in the left hand side of (4), where we know from the definitions of $hidar(G)$, $hidar(G')$ and $E \cap E' = \emptyset$ that $hidar(G)\,hidar(G') = \emptyset = hidar(G')\,hidar(G)$. We abstract a bit and show the following properties.

Lemma 4.3 *Consider relations R, S, T.*

1. $(R \cup S)^+ \;=\; R^+ \,\cup\, R^*\,(S\,R^*)^+$.
2. *If* $R\,S = \emptyset \;=\; S\,R$ *then* $(R \cup S)^+ \;=\; R^+ \,\cup\, S^+$ *and* $(R \cup S)^* \;=\; R^* \,\cup\, S^*$.
3. *If* $R\,S \;=\; \emptyset \;=\; S\,R$ *then* $(R \cup S \cup T)^+ \;=\; R^+ \,\cup\, S^+ \,\cup\, D\,(T\,D)^+$*, where* $D =_{df}\; R^* \,\cup\, S^*$.

For the expression occurring in the left hand side of (4) we obtain from Part 3

$$(hidar(G) \cup hidar(G') \cup C)^+ \;=\; hidar(G)^+ \;\cup\; hidar(G')^+ \;\cup\; D\,(C\,D)^+ \;, \quad (8)$$

where $D \;=\; hidar(G)^* \cup hidar(G')^*$. This is the formal counterpart of the above-mentioned path decomposition.

From this, further intensive use of regular algebra finally leads to a proof of (4), which together with Lm. 4.2 establishes

Theorem 4.4 *For tracelets G, G' with $E \cap E'$ we have*

$$spec(G \mid G') = spec(spec(G) \mid spec(G')) \;.$$

5 The Proofs

5.1 Preliminaries: Subidentity Notation

Since the notation for restrictions used in the main text is calculationally quite unwieldy, we now represent sets of points as *subidentities*, i.e., subsets of the identity relation I between points. Formally, a set $E \subseteq \mathsf{Pt}$ of points is represented by the subidentity $I_E \;=_{df}\; \{(e,e) \,|\, e \in E\}$. The relative complement of a subidentity I_E is $\neg I_E \;=_{df}\; I - I_E$. Relational composition is denoted by juxtaposition. If I_E is a subidentity and A is a binary relation, then $I_E\,A \;=\; A \cap E \times \mathsf{Pt}$ and $A\,I_E \;=\; A \cap \mathsf{Pt} \times E$; these represent represent restriction of A to E on the input and output side, respectively. We recall that for subidentities I_E, I'_E we have $I_E\,I'_E \;=\; I_{E\cap E'}$ and $I_{E-E'} \;=\; I_E\,\neg I'_E$. To save notation, in the sequel we do not distinguish between E and I_E any more.

A main tool in our proofs is

Lemma 5.1 (Restriction Lemma) *For all relations A, B and all subidentities E, E' the following properties hold.*

1. $E\,(A \cap B) \;=\; E\,A \,\cap\, B$.
2. *With $\mathbb{T}$ denoting the universal relation,* $E\,B \;=\; E\,\mathbb{T} \cap B$.
   In particular, $E \;=\; E\,\mathbb{T} \cap I$.
3. $E\,(A \cap B) \;=\; E\,A \,\cap\, E\,B$
4. $E\,E'\,A \;=\; E\,A \,\cap\, E'\,A$.
5. $E\,E' \;=\; \emptyset \;\Longrightarrow\; E\,A \,\cap\, E'\,B \;=\; \emptyset$.

For the proof see [Möl04].

Using subidentity notation, the healthiness condition on tracelets can be reformulated as

$$A \;=\; E\,B \cup B\,E \;,$$

while absence of loose arrows reads

$$\neg E\, A\, \neg E = \emptyset \ .$$

Moreover, the distinguished sets of arrows can be expressed as

$$\begin{array}{lll} hidar(G) & =_{df} & E\, A\, E \ , \\ inar(G) & =_{df} & \neg E\, A\, E \ , \\ outar(G) & =_{df} & E\, A\, \neg E \ . \end{array}$$

It is useful to employ domain and codomain notation for relations A:

$$\begin{array}{lll} \ulcorner A & =_{df} & \{(x,x) \mid \exists\, y : (x,y) \in A\} \ , \\ A\urcorner & =_{df} & \{(y,y) \mid \exists\, x : (x,y) \in A\} \ . \end{array}$$

It will also be useful to introduce the modal operators box and diamond:

$$\begin{array}{lllllll} |A\rangle E & =_{df} & \ulcorner(A\, E) \ , & \qquad & \langle A|E & =_{df} & (E\, A)\urcorner \ , \\ |A]E & =_{df} & \neg|A\rangle\neg E \ , & \qquad & [A| & =_{df} & \neg\langle A|\neg E \ . \end{array}$$

The subidentity $|A]E$ characterises those points for which *all* arrows in A lead to points in E. Therefore we have the following important propagation property:

$$(|A]E)\, A = (|A]E)\, A\, E \ . \tag{9}$$

Then the sets of input and output points of a trace G and their complements can be defined as

$$\begin{array}{lll} in(G) & =_{df} & inar(A)\urcorner = \langle(A\, E)|\neg E \ , \\ out(G) & =_{df} & \ulcorner outar(A) = |(E\, A)\rangle\neg E \ , \\ \neg in(G) & =_{df} & [(A\, E)|E \ , \\ \neg out(G) & =_{df} & |(E\, A)]E \ . \end{array}$$

With our abbreviations this would read more simply as

$$\begin{array}{lll} i & =_{df} & ia\urcorner = \langle(A\, E)|\neg E \ , \\ o & =_{df} & \ulcorner oa = |(E\, A)\rangle\neg E \ , \\ \neg i & =_{df} & [(A\, E)|E \ , \\ \neg o & =_{df} & |(E\, A)]E \ . \end{array} \tag{10}$$

In the sequel, when G is understood, we will use the abbreviations

$$\begin{array}{lllllll} ia & =_{df} & inar(G) \ , & \qquad & i & =_{df} & in(G) \ , \\ oa & =_{df} & outar(G) \ , & \qquad & o & =_{df} & out(G) \ , \\ ha & =_{df} & hidar(G) \ . & & & & \end{array}$$

Decorations of G will be transferred to these abbreviations; e.g. $ia' =_{df} inar(G')$. The same goes for E and A.

5.2 Auxiliary Properties

We start with a few useful properties of the interaction between the trace arrow operators.

Lemma 5.2 *We have the following composition tables; a † sign means that the result holds provided* $i\,o = \emptyset$*; otherwise no simplification is possible.*

	ia	oa
i	$\emptyset$	$\emptyset^\dagger$
$\neg i$	ia	$oa^\dagger$
o	$\emptyset$	oa
$\neg o$	ia	$\emptyset$

	i	$\neg i$	o	$\neg o$
ia	ia	$\emptyset$	$\emptyset^\dagger$	$ia^\dagger$
oa	$\emptyset$	oa	$\emptyset$	oa

Proof. We show a sample calculation.

$$
\begin{array}{ll}
 & o\,ia \\
= & \quad \{\!\![\ \text{definition } o\ ]\!\!\} \\
 & \ulcorner oa\,ia \\
= & \quad \{\!\![\ \text{definitions } ia, oa\ ]\!\!\} \\
 & \ulcorner(E\,A\,\neg E)\,\neg E\,A\,E \\
\leq & \quad \{\!\![\ \text{property of domain and isotony}\ ]\!\!\} \\
 & E\,\neg E\,A\,E \\
= & \quad \{\!\![\ \text{subidentity algebra}\ ]\!\!\} \\
 & \emptyset\,A\,E \\
= & \quad \{\!\![\ \text{strictness}\ ]\!\!\} \\
 & \emptyset\ .
\end{array}
$$

The remaining claims follow analogously. □

5.3 The Proper Proofs I

Proof of (3).
Translated into subidentity notation the property reads

$$\mathrm{AGR}(G, G') \iff E\,A\,E' = E\,A'\,E' \wedge E'\,A\,E = E'\,A'\,E\ .$$

Similarly, saturation (1) reads $A = E\,\mathsf{Dep} \cup \mathsf{Dep}\,E$. Now we calculate as follows.

$$
\begin{array}{ll}
 & E\,A\,E' \\
= & \quad \{\!\![\ \text{by saturation}\ ]\!\!\} \\
 & E\,(E\,\mathsf{Dep} \cup \mathsf{Dep}\,E)\,E' \\
= & \quad \{\!\![\ \text{distributivity}\ ]\!\!\}
\end{array}
$$

$$
\begin{array}{rl}
& E\,E\,\mathsf{Dep}\,E' \,\cup\, E\,\mathsf{Dep}\,E\,E' \\
= & \quad \{\![\ \text{subidentity composition is intersection, and } E \cap E' = \emptyset\ ]\!\} \\
& E\,\mathsf{Dep}\,E' \,\cup\, E\,\mathsf{Dep}\,\emptyset \\
= & \quad \{\![\ \text{strictness and neutrality}\ ]\!\} \\
& E\,\mathsf{Dep}\,E' .
\end{array}
$$

An analogous calculation shows $E\,A'\,E' = E\,\mathsf{Dep}\,E'$, and we are done. $\square$

Proof of Lm. 3.2.
($\Leftarrow$) is immediate by choosing $F = E$ and $F' = E'$.
($\Rightarrow$)

$$
\begin{array}{rl}
& F\,A\,F' \\
= & \quad \{\![\ \text{by } F \subseteq E, F' \subseteq E'\ ]\!\} \\
& F\,E\,A\,E'\,F' \\
= & \quad \{\![\ \text{by AGR}(G, G')\ ]\!\} \\
& F\,E\,A'\,E'\,F' \\
= & \quad \{\![\ \text{by } F \subseteq E, F' \subseteq E'\ ]\!\} \\
& F\,A'\,F' \ .
\end{array}
$$

$\square$

Proof of Thm. 3.1.
For abbreviation we set $\widehat{E} =_{df} i \cup o$, $\widehat{B} =_{df} ia \cup oa$ and $\widehat{A} =_{df} \widehat{B} \cup co$.

1. Concerning the first property we calculate

$$
\begin{array}{rl}
& \widehat{ia} \\
= & \quad \{\![\ \text{definition } \widehat{ia}\ ]\!\} \\
& \neg\widehat{E}\,\widehat{A}\,\widehat{E} \\
= & \quad \{\![\ \text{definition } \widehat{E} \text{ and De Morgan}\ ]\!\} \\
& \neg i\,\neg o\,\widehat{A}\,\widehat{E} \\
= & \quad \{\![\ \text{distributivity, definition of } \widehat{A} \text{ and } co\text{, and Lm. 5.2}\ ]\!\} \\
& ia\,\widehat{E} \\
= & \quad \{\![\ \text{definition of } \widehat{E} \text{ and Lm. 5.2 again}\ ]\!\} \\
& ia \ .
\end{array}
$$

The property $\widehat{oa} = oa$ is shown symmetrically. For the third property we first obtain by the definition of *hidar* and distributivity

$$
hidar(\widehat{G}) = \widehat{E}(\widehat{B} \cup co)\widehat{E} = \widehat{E}\,\widehat{B}\,\widehat{E} \,\cup\, \widehat{E}\,co\,\widehat{E} \ .
$$

For the left summand we continue as follows.

$$
\begin{array}{ll}
 & \widehat{E}\,\widehat{B}\,\widehat{E} \\
= & \quad \{\![\text{ definitions and distributivity }]\!\} \\
 & (i\,ia \cup i\,oa \cup o\,ia \cup o\,oa)\,\widehat{E} \\
= & \quad \{\![\text{ Lm. 5.2 }]\!\} \\
 & (\emptyset \cup i\,oa \cup \emptyset \cup oa)\,\widehat{E} \\
= & \quad \{\![\text{ neutrality of } \emptyset \text{ and } i\,oa \subseteq oa \text{ by } i \subseteq I\ ]\!\} \\
 & oa\,\widehat{E} \\
= & \quad \{\![\text{ Lm. 5.2 again }]\!\} \\
 & \emptyset\ .
\end{array}
$$

For the second summand we obtain by the definitions and the absorption laws

$$\widehat{E}\,co\,\widehat{E} = (i \cup o)\,i\,ha^+\,o\,(i \cup o) = i\,ha^+\,o = co\ .$$

2. The properties of $\widehat{i}$ and $\widehat{o}$ are immediate from the ones of $\widehat{ia}$ and $\widehat{oa}$ in Part 1 and the definitions of i and o.
3. Immediate from the first two parts and the fact that a tracelet is uniquely determined by its *inar*, *outar* and *hidar* sets. □

Proof of Lm. 3.3.
For the first property we reason as follows.

$$
\begin{array}{ll}
 & \widehat{ia} \\
= & \quad \{\![\text{ definitions }]\!\} \\
 & \neg(E \cup E')\,(A \cup A')\,(E \cup E') \\
= & \quad \{\![\text{ De Morgan }]\!\} \\
 & \neg E\,\neg E'\,(A \cup A')\,(E \cup E') \\
= & \quad \{\![\text{ distributivity }]\!\} \\
 & \neg E\,\neg E'\,A\,E \,\cup\, \neg E\,\neg E'\,A\,E' \,\cup\, \neg E\,\neg E'\,A'\,E \,\cup\, \neg E\,\neg E'\,A'\,E' \\
= & \quad \{\![\text{ commutatibility of subidentities }]\!\} \\
 & \neg E'\,\neg E\,A\,E \,\cup\, \neg E'\,\neg E\,A\,E' \,\cup\, \neg E\,\neg E'\,A'\,E \,\cup\, \neg E\,\neg E'\,A'\,E' \\
= & \quad \{\![\text{ definition of } inar,\ E \subseteq \neg E',\ E' \subseteq \neg E \text{ and (2) }]\!\} \\
 & \neg E'\,ia \,\cup\, \neg E'\,\emptyset \,\cup\, \neg E\,\emptyset \,\cup\, \neg E\,ia' \\
= & \quad \{\![\text{ strictness and neutrality }]\!\} \\
 & \neg E'\,ia \,\cup\, \neg E\,ia'\ .
\end{array}
$$

The proof of the second property is symmetric to that of the first one. The claims about *in* and *out* are straightforward from the definitions.

For the last property we first calculate

$$
\begin{array}{ll}
 & \widehat{ha} \\
= & \quad \{\![\text{ definitions }]\!\}
\end{array}
$$

$$
\begin{array}{ll}
& (E \cup E')\,(A \cup A')\,(E \cup E') \\
= & \quad \{\![\text{ distributivity }]\!\} \\
& E\,A\,E \,\cup\, E\,A\,E' \,\cup\, E\,A'\,E \,\cup\, E\,A'\,E' \,\cup \\
& E'\,A\,E \,\cup\, E'\,A\,E' \,\cup\, E'\,A'\,E \,\cup\, E'\,A'\,E' \\
= & \quad \{\![\text{ definition of } \mathit{hidar},\ E \subseteq \neg E',\ E' \subseteq \neg E \text{ and (2) }]\!\} \\
& \widehat{ia} \,\cup\, E\,A\,E' \,\cup\, \emptyset \,\cup\, E\,A'\,E' \,\cup\, E'\,A\,E \,\cup\, \emptyset \,\cup\, E'\,A'\,E \,\cup\, \widehat{ia}' \\
= & \quad \{\![\text{ strictness and neutrality }]\!\} \\
& \widehat{ia} \,\cup\, E\,A\,E' \,\cup\, E\,A'\,E' \,\cup\, E'\,A\,E \,\cup\, E'\,A'\,E \,\cup\, \widehat{ia}' \\
= & \quad \{\![\text{ assumption } \mathrm{AGR}(G, G')]\!\} \\
& \widehat{ia} \,\cup\, E\,A\,E' \,\cup\, E'\,A\,E \,\cup\, \widehat{ia}'\ .
\end{array}
$$

Hence it remains to show $E\,A\,E' \,\cup\, E'\,A\,E \,=\, A \cap A'$. We have

$$
\begin{array}{ll}
& A \cap A' \\
= & \quad \{\![\text{ definitions }]\!\} \\
& (ia \cup ha \cup oa) \cap (ia' \cup ha' \cup oa') \\
= & \quad \{\![\text{ distributivity and Lm. 5.4 }]\!\} \\
& (ia \cap oa') \,\cup\, (ia' \cap oa) \\
= & \quad \{\![\text{ definitions }]\!\} \\
& (\neg E\,A\,E \,\cap\, E'\,A'\,\neg E') \,\cup\, (E\,A\,\neg E \,\cap\, \neg E'\,A'\,E') \\
= & \quad \{\![\text{ Restriction Lemma and } E \subseteq \neg E',\ E' \subseteq \neg E]\!\} \\
& E'\,(A \cap A')\,E \,\cup\, E\,(A \,\cap\, A')\,E' \\
= & \quad \{\![\text{ Restriction Lemma }]\!\} \\
& (E'\,A\,E \,\cap\, E'\,A'\,E) \,\cup\, (E\,A\,E' \,\cap\, E\,A'\,E') \\
= & \quad \{\![\text{ assumption } \mathrm{AGR}(G, G')]\!\} \\
& E'\,A\,E \,\cup\, E\,A\,E'\ .
\end{array}
$$

□

Proof of Lm. 3.4. We use the same notation as in the proof of Thm. 3.1 and set $\widehat{G} =_{df}\ \mathit{spec}(G) = (\widehat{E}, \widehat{A})$ with $\widehat{E} =_{df}\ i \cup o$, $\widehat{B} =_{df}\ ia \cup oa$ and $\widehat{A} =_{df}\ \widehat{B} \cup co$; like wise for G'.

We calculate now the interface arrows for $\widetilde{G} =_{df}\ \widehat{G} \circ \widehat{G}'$.

$$
\begin{array}{ll}
& \mathit{inar}(\widetilde{G}) \\
= & \quad \{\![\text{ Lm. 3.3 }]\!\} \\
& \neg\widehat{E}'\,\mathit{inar}(\widehat{G}) \,\cup\, \neg\widehat{E}\,\mathit{inar}(\widehat{G}') \\
= & \quad \{\![\text{ Thm. 3.1 }]\!\} \\
& \neg\widehat{E}'\,ia \,\cup\, \neg\widehat{E}\,ia' \\
= & \quad \{\![\text{ definitions }]\!\} \\
& \neg(i' \cup o')\,ia \,\cup\, \neg(i \cup o)\,ia'
\end{array}
$$

$$
\begin{array}{ll}
= & \{\![\text{ De Morgan }]\!\} \\
 & \neg i' \, \neg o' \, ia \cup \neg i \, \neg o \, ia' \\
= & \{\![\text{ commutativity of subidentities and Lm. 5.3 }]\!\} \\
 & \neg i' \, ia \cup \neg i \, ia' \\
= & \{\![\text{ Lm. 3.3 }]\!\} \\
 & inar(G \mid G') \ .
\end{array}
$$

An analogous calculation shows

$$outar(\widetilde{G}) = outar(G \mid G') \ .$$

□

5.4 Further Auxiliary Properties

As before we also investigate the interaction of the sets of input and output points with the arrow sets in a composition.

Lemma 5.3 *Assume $E \cap E' = \emptyset$. We have the following composition tables. A sign † means that the result holds provided* AGR(G, G')*, while a dash means that no simplification is possible in that case.*

	ia'	oa'
i	$-$	$\emptyset$
$\neg i$	$-$	$\neg oa'$ †
o	$-$	$\emptyset$
$\neg o$	ia' †	$-$

	i	$\neg i$	o	$\neg o$
ia'	$\emptyset$	ia'	$\emptyset$	ia'
oa'	$-$	oa	$-$	oa

Proof. As a sample we show $i \, oa' = \emptyset$. The remaining proofs are similar.

Using the definitions of i and oa' together with $E \, E' = \emptyset$ we have

$$i \, oa' \ = \ i \, E' \, A' \, \neg E' \ \subseteq \ E \, E' \, A' \, \neg E' \ = \ \emptyset \, A' \, \neg E' \ = \ \emptyset \ .$$

□

Next, we give an intersection table for the various arrow sets involved. A dash means that no simplification is possible in that case.

Lemma 5.4 *For arbitrary G, G' with $E \cap E' = \emptyset$,*

$\cap$	ia	ha	oa	co
ia'	$\emptyset$	$\emptyset$	$-$	$\emptyset$
ha'	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
oa'	$-$	$\emptyset$	$\emptyset$	$\emptyset$
co'	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$

The proofs are straightforward from the definitions and the Restriction Lemma 5.1.

Corollary 5.5 *Under the above assumptions* $A \cap A' = (ia' \cap oa) \cup (ia \cap oa')$.

As a further preparation we show that the AGR predicate is compatible with *spec*.

Lemma 5.6 *If* $\mathrm{AGR}(G, G')$ *then also* $\mathrm{AGR}(\mathit{spec}(G), \mathit{spec}(G'))$.

Proof. As before we use the abbreviations $\widehat{G} =_{df} \mathit{spec}(G)$ etc. Assuming $\mathrm{AGR}(G, G')$ we have to prove $\widehat{E}\,\widehat{A}\,\widehat{E}' = \widehat{E}\,\widehat{A}\,\widehat{E}'$ and $\widehat{E}'\,\widehat{A}\,\widehat{E} = \widehat{E}'\,\widehat{A}\,\widehat{E}$. We only show the first equation, the second one is symmetric. We have

$$
\begin{array}{ll}
 & \widehat{E}\,\widehat{A}\,\widehat{E}' \\
= & \quad \{\!\![\text{ definitions }]\!\!\} \\
 & \widehat{E}\,(ia \cup oa \cup co)\,\widehat{E}' \\
= & \quad \{\!\![\text{ distributivity }]\!\!\} \\
 & \widehat{E}\; ia\;\widehat{E}' \cup \widehat{E}\; oa\;\widehat{E}' \cup \widehat{E}\; co\;\widehat{E}'\,\widehat{E}' \\
= & \quad \{\!\![\text{ composition tables }]\!\!\} \\
 & \emptyset \cup \widehat{E}\; oa\;\widehat{E}' \cup \emptyset \\
= & \quad \{\!\![\text{ neutrality of } \emptyset \text{ and definition } oa \;]\!\!\} \\
 & \widehat{E}\,E\,A\,\neg E\,\widehat{E}' \\
= & \quad \{\!\![\text{ since } \widehat{E} \subseteq E \text{ and } \widehat{E}' \subseteq E' \subseteq \neg E \;]\!\!\} \\
 & \widehat{E}\,A\,\widehat{E}' \;.
\end{array}
$$

Similarly,

$$
\begin{array}{ll}
 & \widehat{E}\,\widehat{A}'\,\widehat{E}' \\
= & \quad \{\!\![\text{ definitions }]\!\!\} \\
 & \widehat{E}\,(ia' \cup oa' \cup co')\,\widehat{E}' \\
= & \quad \{\!\![\text{ distributivity }]\!\!\} \\
 & \widehat{E}\; ia'\;\widehat{E}' \cup \widehat{E}\; oa'\;\widehat{E}' \cup \widehat{E}\; co'\;\widehat{E}'\,\widehat{E}' \\
= & \quad \{\!\![\text{ composition tables }]\!\!\} \\
 & \widehat{E}\; ia'\;\widehat{E}' \cup \emptyset \cup \emptyset \\
= & \quad \{\!\![\text{ neutrality of } \emptyset \text{ and definition } ia' \;]\!\!\} \\
 & \widehat{E}\,\neg E'\,A'\,E'\,\widehat{E}' \\
= & \quad \{\!\![\text{ since } \widehat{E}' \subseteq E' \text{ and } \widehat{E} \subseteq E \subseteq \neg E' \;]\!\!\} \\
 & \widehat{E}\,A'\,\widehat{E}' \;.
\end{array}
$$

Now Lm. 3.2 with $\widehat{E} \subseteq E$ and $\widehat{E}' \subseteq E'$ shows $\widehat{E}\,A\,\widehat{E}' = \widehat{E}\,A'\,\widehat{E}'$, and we are done. $\square$

5.5 The Proper Proofs II

Proof of Thm. 4.1.
We use the same abbreviations as in the proof of Thm. 3.1. By Thm. 3.1 it suffices to analyse the hidden arrows. We calculate as follows.

$$\begin{array}{ll} & co\ co \\ = & \quad \{\!\![\ \text{definition of } co\ ]\!\!\} \\ & i\ ha^+\ o\ i\ ha^+\ o \\ \subseteq & \quad \{\!\![\ i, o \subseteq I\ ]\!\!\} \\ & i\ ha^+\ ha^+\ o \\ \subseteq & \quad \{\!\![\ \text{transitivity of } ha^+\ ]\!\!\} \\ & i\ ha^+ o \\ = & \quad \{\!\![\ \text{definition of } co\ ]\!\!\} \\ & co\ . \end{array}$$

Therefore co is transitive and hence $\widehat{ha}^+ = co^+ = co$. This finishes the proof. □

Proof of Lm. 4.2.

1. Set $\widehat{B} =_{df} inar(G) \cup outar(G)$, and likewise for $\widehat{B}'$. By the definitions and distributivity,

   $$\widehat{A} \cap \widehat{A}' = (\widehat{B} \cup co) \cap (\widehat{B}' \cup co') = (\widehat{B} \cap \widehat{B}') \cup (\widehat{B} \cap co') \cup (co \cap \widehat{B}') \cup (co \cap co')\ .$$

   The last three summands are $\emptyset$ by Lm. 5.4. For the first one we calculate as follows.

   $$\begin{array}{ll} & \widehat{B} \cap \widehat{B}' \\ = & \quad \{\!\![\ \text{definitions}\ ]\!\!\} \\ & (ia \cup oa) \cap (ia' \cup oa') \\ = & \quad \{\!\![\ \text{distributivity}\ ]\!\!\} \\ & (ia \cap ia') \cup (ia \cap oa') \cup (oa \cap ia') \cup (oa \cap oa') \\ = & \quad \{\!\![\ \text{Lm. } 5.4\ ]\!\!\} \\ & \emptyset \cup (ia \cap oa') \cup (oa \cap ia') \cup \emptyset \\ = & \quad \{\!\![\ \text{neutrality of } \emptyset \text{ and Cor. } 5.5\ ]\!\!\} \\ & A \cap A'\ . \end{array}$$

2. From Lm. 5.6 we know $\mathrm{AGR}(spec(G), spec(G'))$. Hence

   $$\begin{array}{ll} & hidar(\widehat{G} \mid \widehat{G}') \\ = & \quad \{\!\![\ \text{Lm. } 3.3\ ]\!\!\} \\ & \widehat{ha} \cup \widehat{ha}' \cup (\widehat{A} \cap \widehat{A}') \end{array}$$

$$
\begin{array}{ll}
= & \quad \{\![\text{ Thm. 4.1 }]\!\} \\
 & co \cup co' \cup (\widehat{A} \cap \widehat{A}') \\
= & \quad \{\![\text{ Part 1 }]\!\} \\
 & co \cup co' \cup (A \cap A') \ .
\end{array}
$$

3. For abbreviation we set $C =_{df} A \cap A'$, $\widetilde{ha} =_{df} hidar(G \mid G')$ and $\widetilde{\widehat{ha}} =_{df} hidar(\widehat{G} \mid \widehat{G}')$.
   Since $i, o, i', o' \subseteq I$ we have $co = i\, ha^+\, o \subseteq ha^+$ and likewise $co' \subseteq ha'^+$. Therefore,

$$
\begin{array}{ll}
 & \widetilde{\widehat{ha}} \\
= & \quad \{\![\text{ Part 2 }]\!\} \\
 & co \cup co' \cup C \\
\subseteq & \quad \{\![\text{ above remark }]\!\} \\
 & ha^+ \cup ha'^+ \cup C \\
\subseteq & \quad \{\![\ C \subseteq C^+ \text{ and isotony of } {}^+ \ ]\!\} \\
 & (ha \cup ha' \cup C)^+ \\
= & \quad \{\![\text{ Lm. 3.3 }]\!\} \\
 & \widetilde{ha}^+ \ .
\end{array}
$$

   Now we obtain, again by isotony of $^+$ and by standard regular algebra,

$$\widetilde{\widehat{ha}}^+ \subseteq (\widetilde{ha}^+)^+ \subseteq \widetilde{ha}^+$$

   and therefore, with $\tilde{i} =_{df} i \cup i'$ and $\tilde{o} =_{df} o \cup o'$, by Lm. 3.3,

$$hidar(spec(\widehat{G} \mid \widehat{G}')) = \tilde{i}\, \widetilde{\widehat{ha}}^+\, \tilde{o} \subseteq \tilde{i}\, \widetilde{ha}^+\, \tilde{o} = hidar(spec(G \mid G')) \ .$$

□

Proof of Lm. 4.3.

1.
$$
\begin{array}{ll}
 & (R \cup S)^+ \\
= & \quad \{\![\text{ (5) }]\!\} \\
 & (R \cup S)\,(R \cup S)^* \\
= & \quad \{\![\text{ star of sum }]\!\} \\
 & (R \cup S)\, R^*\, (S\, R^*)^* \\
= & \quad \{\![\text{ distributivity }]\!\} \\
 & R\, R^*\, (S\, R^*)^* \ \cup\ S\, R^*\, (S\, R^*)^* \\
= & \quad \{\![\text{ (5) }]\!\}
\end{array}
$$

$$
\begin{array}{ll}
& R^+ (S\,R^*)^* \cup (S\,R^*)^+ \\
= & \quad \{\!\!\{ \ (**) \text{ applied to } (S\,R^*)^*, \text{ distributivity and neutrality of } I \ \}\!\!\} \\
& R^+ \cup R^+ (S\,R^*)^+ \cup (S\,R^*)^+ \\
= & \quad \{\!\!\{ \text{ neutrality of } I \text{ and distributivity } \}\!\!\} \\
& R^+ \cup (R^+ \cup I)\,(S\,R^*)^+ \\
= & \quad \{\!\!\{ \ (5) \ \}\!\!\} \\
& R^+ \cup R^* \,(S\,R^*)^+ \ .
\end{array}
$$

2. By (6) and (5), distributivity and neutrality of I, the assumption $S\,R = \emptyset$ and strictness of relational composition,

$$S\,R^* \;=\; S\,(I \cup R\,R^*) \;=\; S \cup S\,R\,R^* \;=\; S \ .$$

Hence by the above, (6) and (5), distributivity and neutrality of I, the assumption $R\,S = \emptyset$ and strictness of relational composition,

$$R^*\,(S\,R^*)^+ \;=\; R^*\,S^+ \;=\; (I \cup R^*\,R)\,S\,S^* \;=\; S\,S^* \;=\; S^+ \ ,$$

which together with Part 1 shows the first claim. The second one is immediate from that by (6), idempotence of $\cup$ and (6) again.

3. Immediate from the two previous parts. □

We need another auxiliary result that connects the arrow set C with input and output points.

Lemma 5.7 $C \;=\; \tilde{i}\,C \;=\; \tilde{o}\,C \;=\; C\,\tilde{i} \;=\; C\,\tilde{o}$.

The proof is immediate from the composition tables in Lm. 5.3 together with Lm. 5.1.1.

Proof of Eq. (4)
We start with the left hand side of (4). By idempotence of subidentities, distributivity and Lm. 4.3.3 we obtain

$$
\begin{aligned}
\tilde{i}\,(ha \cup ha' \cup C)^+\,\tilde{o} &= \tilde{i}\,(\tilde{i}\,ha^+\,\tilde{o} \cup \tilde{i}\,ha'^+\,\tilde{o} \cup \tilde{i}\,D\,(C\,D)^+\,\tilde{o})\,\tilde{o} \\
&= \tilde{i}\,(co \,\cup\, co' \,\cup\, \tilde{i}\,D\,(C\,D)^+\,\tilde{o})\,\tilde{o} \ .
\end{aligned}
\tag{11}
$$

We transform the third summand within the parentheses further.

$$
\begin{array}{ll}
& \tilde{i}\,D\,(C\,D)^+\,\tilde{o} \\
= & \quad \{\!\!\{ \ (5) \ \}\!\!\} \\
& \tilde{i}\,D\,(C\,D)^*\,C\,D\,\tilde{o} \\
= & \quad \{\!\!\{ \text{ Lm. 5.7 } \}\!\!\}
\end{array}
$$

$$
\begin{array}{cl}
 & \tilde{\tilde{i}}\, D\, (\tilde{o}\, C\, \tilde{\tilde{i}}\, D)^*\, \tilde{o}\, C\, \tilde{\tilde{i}}\, D\, \tilde{o} \\
= & \quad \{\!\![\text{ star shift rule } R\,(S\,R)^* \;=\; (R\,S)^*\,R \;]\!\!\} \\
 & (\tilde{\tilde{i}}\, D\, \tilde{o}\, C)^*\, \tilde{\tilde{i}}\, D\, \tilde{o}\, C\, \tilde{\tilde{i}}\, D\, \tilde{o} \\
= & \quad \{\!\![\text{ abbreviation } D^\circ \;=_{df}\; \tilde{\tilde{i}}\, D\, \tilde{o} \text{ and } (*) \;]\!\!\} \\
 & (D^\circ\, C)^*\, D^\circ\, C\, D^\circ \\
= & \quad \{\!\![\text{ star shift }]\!\!\} \\
 & D^\circ\, (C\, D^\circ)^*\, C\, D^\circ \\
= & \quad \{\!\![\text{ (5) }]\!\!\} \\
 & D^\circ\, (C\, D^\circ)^+ \;.
\end{array}
$$

We can simplify this using distributivity, (5) and Lm. 5.3:

$$D^\circ \;=\; i\; ha^+\; o \cup i'\; ha'^+\; o' \;=\; co \cup co' \;.$$

We note that

$$co\; co' = \emptyset = co'\; co \;, \tag{12}$$

since by the definitions and $E\,E' = \emptyset$ we have

$$co\; co' = i\; ha^+\; o\; i'\; ha'^+\; o' \subseteq i\; ha^+\; E\,E'\; ha'^+\; o' = i\; ha^+\; \emptyset\; ha'^+\; o' = \emptyset \;,$$

and symmetrically for the second equation.

Now we can finish our derivation:

$$
\begin{array}{cl}
 & \tilde{\tilde{i}}\, (ha \cup ha' \cup C)^+\, \tilde{o} \\
= & \quad \{\!\![\text{ (11) }]\!\!\} \\
 & \tilde{\tilde{i}}\, (co \;\cup\; co' \;\cup\; \tilde{\tilde{i}}\, D\, (C\, D)^+\, \tilde{o}))\, \tilde{o} \\
= & \quad \{\!\![\text{ above calculations }]\!\!\} \\
 & \tilde{\tilde{i}}\, (co \cup co' \cup (co \cup co')\, (C\, (co \cup co'))^+)\, \tilde{o} \\
\subseteq & \quad \{\!\![\; R \subseteq R^* \text{ and isotony }]\!\!\} \\
 & \tilde{\tilde{i}}\, (co \cup co' \cup (co \cup co')^*\, (C\, (co \cup co')^*)^+)\, \tilde{o} \\
= & \quad \{\!\![\text{ (12), Lm. 4.3.3, since } co\; co' \;=\; \emptyset \;=\; co'\; co \text{ by Lm. 5.4,} \\
 & \quad\;\; \text{and distributivity }]\!\!\} \\
 & \tilde{\tilde{i}}\, (co \;\; \cup co' \cup C)^+\, \tilde{o} \;,
\end{array}
$$

as claimed. □

References

1. B. Möller, C.A.R. Hoare, M.E. Müller, G. Struth: A discrete geometric model of concurrent program execution. In H. Zhu, J. Bowen: Proc. UTP 16. LNCS 10134. Springer 2017, 1–25
2. T. Hoare, S. van Staden, B. Möller, G. Struth, H. Zhu: Developments in concurrent Kleene algebra. Journal of Logical and Algebraic Methods in Programming, 85(4), 617–636 (2016)