

Towards Bialgebraic Semantics for CSP

Technical Report FCT/UNL-DI 3-2010
(Draft)

Ana Paula Maldonado¹, Luís Monteiro¹, and Markus Roggenbach²

¹ CITI, Departamento de Informática, Faculdade de Ciências e Tecnologia,
Universidade Nova de Lisboa, 2829-516 Caparica, Portugal

² Swansea University, Wales, UK

Abstract. This paper extends bialgebraic semantics [1, 2] to take into account notions of behaviour that lead to process equivalences coarser than bisimulation. For that purpose, the requirement of finality for the characterisation of behaviours is relaxed to quasi-finality, which informally consists in relegating to the underlying category the conditions that finality must satisfy in the main category of coalgebras. This setting is then applied to the failure semantics of CSP.

1 Introduction

Giving semantics to process algebra in the form of SOS has become standard since Plotkin's seminal paper [3]. Besides the transition system of a process, however, one is often interested in a more abstract description of a process, based on observations such as traces or failures. Naturally, this leads to the questions of how to obtain observations from a transition system. This can be done via an algebraic approach using initiality of the term algebra, or coalgebraically via finality of the intended observational model.

Bi-algebras [1, 2] host these two approaches within one framework, and allow to study conditions under which they are equal. In this paper we are interested in observations that lead to notions of process equivalence coarser than bisimulation. This is motivated, e.g., by the various semantics of the process algebra CSP [4, 5], which lie within the linear time (trace semantics) – branching time (bisimulation semantics) spectrum [6]. As final objects are unique up to isomorphisms, any given category can cater for just one semantics given by finality. If one is interested in various semantics for one process algebra – as is, e.g., the case for CSP – there are two possible approaches: either one defines a specialized category for each semantic model, or, one relaxes the requirement of finality. Here, we follow the latter approach and relax finality to quasi-finality [7, 8]. Briefly, quasi-finality has a characterisation similar to that of finality, except that the defining conditions are required to hold only in the underlying category (of sets and functions, for simplicity) rather than in the category of coalgebras.

Relatively to a functor B describing the type of transition structure, we introduce the notion of an observational model. Such a model consists of observations, e.g. trace languages. These observations carry a transition structure of type B .

In the case of trace languages, for instance, it is natural to define $L \xrightarrow{a} L'$ if $\langle a \rangle \in L$ and $L' = \{x \mid \langle a \rangle \hat{x} \in L\}$. Additionally, an observational model defines an observation function from any B -coalgebra to the set of observations of the model. Furthermore, the observational model is required to be quasi-final in the category of B -coalgebras w.r.t. these observation functions.

With these notions we obtain: Given the signature Σ of a process algebra P and its transition rules in (abstract) GSOS format [9, 2] for a functor B , and given an observational model for the same functor B , the operational semantics of P is the observation function, from the coalgebra defined by the transition rules, into the observation model. All operators of Σ are defined on the observation model by quasi-finality. The denotational semantics of P is defined by initiality of the term algebra. When the observational model is a final coalgebra, the operational and the denotational semantics are automatically equivalent if the transition rules are in some “well-behaved” format like (abstract) GSOS format. We currently do not know whether the same is true for quasi-final observational models. A sufficient condition for the equivalence of the semantics is that a certain observation function is an algebra homomorphism, but in the current state of our knowledge we have to check this for every operator in the signature.

In our view one of the advantages of the present approach is that both the operational and the denotational semantics are defined in terms of the transition rules for the (operators representing the) constructions of the language, which therefore completely determine the meaning of the language. We illustrate this point by showing how this setting can be applied to define the failure semantics of CSP.

Related work includes alternative coalgebraic characterisations of linear time semantics [10, 11, 12], bialgebraic and modal logic characterisations of process equivalences [13] and coalgebraic models of CSP [14, 15].

2 Bialgebraic Semantics Based on Quasi-Finality

In this section we present the theoretical framework that will be applied in the next section to the semantics of CSP. Our presentation is at the abstraction level of [1]—which is quite appropriate for our purposes in this paper—rather than the more abstract level of [2]. In this section we shall use as a running example a small subset of CSP described by the grammar

$$\begin{aligned}
 P ::= & \text{STOP} && (\text{null}) \\
 & | a \rightarrow P && (\text{action prefix}) \\
 & | P \square P && (\text{external choice}) \\
 & | P ||| P && (\text{interleaving})
 \end{aligned}$$

where a is an action chosen from some given set A .

2.1 Algebras and Syntax

We assume given a (one-sorted) signature Σ that will be fixed throughout. The intention is that the operators in Σ represent the forms of expression of the syn-

tax, the expressions themselves being identified with the Σ -terms. For example, the signature of our small CSP fragment has operators $STOP$ of arity 0, $a \rightarrow (-)$ for all $a \in A$ of arity 1, and \square and \parallel of arity 2.

In the sequel it is useful to use the categorical definition of Σ -algebra. It is a pair $\langle M, \mu \rangle$ where M is a set and μ is a function $\mu : \Sigma M \rightarrow M$. Here we overloaded the notation a bit and treated Σ as the functor defined on sets X by

$$\Sigma X = \coprod_{\sigma \in \Sigma} X^{\text{arity } \sigma} = \{ \langle \sigma, x_1, \dots, x_n \rangle : \sigma \in \Sigma, \text{arity } \sigma = n, x_1, \dots, x_n \in X \}.$$

The operation $\sigma_M : M^n \rightarrow M$ associated with $\sigma \in \Sigma$ of arity n is then given by $\sigma_M(m_1, \dots, m_n) = \mu(\langle \sigma, m_1, \dots, m_n \rangle)$. A homomorphism from $\langle M, \mu \rangle$ to another Σ -algebra $\langle M', \mu' \rangle$, or Σ -homomorphism, is a function $f : M \rightarrow M'$ such that the following diagram commutes:

$$\begin{array}{ccc} \Sigma M & \xrightarrow{\Sigma f} & \Sigma M' \\ \mu \downarrow & & \downarrow \mu' \\ M & \xrightarrow{f} & M'. \end{array}$$

The set $T0$ of Σ -terms can be turned into a Σ -algebra $\langle T0, \alpha_0 \rangle$ by defining $\alpha_0(\langle \sigma, t_1, \dots, t_n \rangle) = \sigma(t_1, \dots, t_n)$ where $\sigma \in \Sigma$ has arity n and t_1, \dots, t_n are terms; this is the initial Σ -algebra: there is a unique Σ -homomorphism ι_M from $\langle T0, \alpha_0 \rangle$ to any Σ -algebra $\langle M, \mu \rangle$.

The free Σ -algebra generated by a set X is defined similarly; it will be denoted $\langle TX, \alpha_X \rangle$, with ‘inclusion of generators’ $\eta_X : X \rightarrow TX$; this notation is compatible with the one for the initial algebra by taking 0 to denote the empty set. The characterising property here is that any function $f : X \rightarrow M$ has a unique extension to a Σ -homomorphism from $\langle TX, \alpha_X \rangle$ to $\langle M, \mu \rangle$. This may be visualised in the following commutative diagram:

$$\begin{array}{ccccc} X & \xrightarrow{\eta_X} & TX & \xleftarrow{\alpha_X} & \Sigma TX \\ & \searrow f & \downarrow f & & \downarrow \Sigma f \\ & & M & \xleftarrow{\mu} & \Sigma M. \end{array}$$

2.2 Coalgebras

With the coalgebras the intention is to capture the dynamics of the expressions of the language. The notion of coalgebra is dual to that of algebra. Given an endofunctor B on the category **Sets** of sets and functions,³ a B -coalgebra is a pair $\langle S, \varphi \rangle$ where S is a set and $\varphi : S \rightarrow BS$ is a function, called the transition

³ The general notions presented here remain valid if we replace **Sets** by an arbitrary category **C**.

structure of the coalgebra. A B -morphism from $\langle S, \varphi \rangle$ to $\langle S', \varphi' \rangle$ is function $f : S \rightarrow S'$ such that $\varphi' \circ f = Bf \circ \varphi$:

$$\begin{array}{ccc} S & \xrightarrow{f} & S' \\ \varphi \downarrow & & \downarrow \varphi' \\ BS & \xrightarrow{Bf} & BS' . \end{array}$$

In this paper our main examples of coalgebras are the (image finite) labelled transition systems, whose definition we now recall. We assume a set A of actions has been fixed. Then a labelled transition system (LTS) is a pair $\langle S, \rightarrow \rangle$ where S is a set and \rightarrow is a subset of $S \times A \times S$; as usual, $(s, a, s') \in \rightarrow$ is written $s \xrightarrow{a} s'$. A LTS $\langle S, \rightarrow \rangle$ will be identified with a coalgebra $\langle S, \varphi \rangle$ for the functor $B = \mathcal{P}(-)^A$; the structure function $\varphi : S \rightarrow \mathcal{P}(S)^A$ is defined by $\varphi(s)(a) = \{s' : s \xrightarrow{a} s'\}$; conversely, given such a coalgebra, the corresponding transition relation is defined by $s \xrightarrow{a} s'$ iff $s' \in \varphi(s)(a)$; the two notations will be used interchangeably. A LTS is image-finite if $\varphi(s)(a)$ is a finite set for all s and a ; in that case we may restrict ourselves to coalgebras with $\varphi : S \rightarrow \mathcal{P}_{\text{fin}}(S)^A$, where \mathcal{P}_{fin} is the finite powerset functor; the reason for doing so is that there is a final coalgebra for the functor $\mathcal{P}_{\text{fin}}(-)^A$, which is not the case for $\mathcal{P}(-)^A$. The general notion of coalgebra morphism $f : S \rightarrow S'$ may be expressed for LTS's by two conditions: (i) if $s \xrightarrow{a} s'$ in S , then $f(s) \xrightarrow{a} f(s')$ in S' ; (ii) whenever $f(s) \xrightarrow{a} t'$ in S' , there is $s' \in S$ such that $s \xrightarrow{a} s'$ in S and $f(s') = t'$. For the failure semantics of CSP in the next section we need to consider LTS's with τ -transitions $s \xrightarrow{\tau} s'$ corresponding to an inner activity of the system in question, but for the moment we will ignore them.

2.3 Transition Structure on Terms

Given functors Σ and B as above, the next step is to define a transition structure on the set $T0$ of terms. The standard way to proceed is to define a LTS with labels in some set A of actions and states in the set $T0$ of terms; the transition relation is specified by SOS rules in the style first advocated by Plotkin [3]. This is the approach followed by Rutten and Turi in [1]. In our running example, the specification rules appear in Figure 1.

In general we need to define a transition structure not only in $T0$ but also in the free algebra TS where S is the underlying set of a B -coalgebra $\langle S, \varphi \rangle$. And this in a way such that the unique Σ -homomorphism $\nu_{TS} : T0 \rightarrow TS$ given by the initiality of $T0$ is also a morphism of B -coalgebras, and similarly for the inclusion of generators $\eta_S : S \rightarrow TS$. In the case of LTSs, the transition structure on TS is specified by the set of rules $R \cup R_S$ where R is the set of rules for the operators in Σ and R_S is just the set of all transitions in S turned into rules with no premisses. For rules in “well-behaved” formats it is guaranteed that ν_{TS} and η_S are indeed B -morphisms (in [1] this was shown for the *tyft/tyxt* format [16]).

$$\begin{array}{l}
\text{Action prefix:} \quad \frac{}{(a \rightarrow P) \xrightarrow{a} P} \\
\text{External choice:} \quad \frac{P \xrightarrow{a} P'}{P \square Q \xrightarrow{a} P'} \qquad \frac{Q \xrightarrow{a} Q'}{P \square Q \xrightarrow{a} Q'} \\
\text{Interleaving:} \quad \frac{P \xrightarrow{a} P'}{P \parallel Q \xrightarrow{a} P' \parallel Q} \qquad \frac{Q \xrightarrow{a} Q'}{P \parallel Q \xrightarrow{a} P \parallel Q'}
\end{array}$$

Fig. 1. SOS rules for the fragment of CSP.

A more abstract approach was proposed by Turi and Plotkin [2]; we shall illustrate the approach with our running example. We can reformulate the rules in Figure 1 to define directly the transition map $S \rightarrow \mathcal{P}_{\text{fin}}(S)^A$, or rather its graph, whose pairs we write in the form $P \mapsto f$ for readability. The new rules are depicted in Figure 2, where an informal lambda notation was used for function definition.

$$\begin{array}{l}
\text{Null:} \quad \frac{}{STOP \mapsto \lambda a. \emptyset} \\
\text{Action prefix:} \quad \frac{}{(a \rightarrow P) \mapsto \lambda b. \begin{cases} \{P\} & \text{if } b = a \\ \emptyset & \text{if } b \neq a \end{cases}} \\
\text{External choice:} \quad \frac{P \mapsto f \quad Q \mapsto g}{P \square Q \mapsto \lambda a. f(a) \cup g(a)} \\
\text{Interleaving:} \quad \frac{P \mapsto f \quad Q \mapsto g}{P \parallel Q \mapsto \lambda a. \{P' \parallel Q : P' \in f(a)\} \cup \{P \parallel Q' : Q' \in g(a)\}}
\end{array}$$

Fig. 2. Inductive definition of the transition map.

Each rule has as many premisses as the arity of the main operator of the rule,⁴ and in fact can be seen as specifying a function of that arity on $TS \times BTS$ with values again in $TS \times BTS$. Actually, it is enough to consider the values in BTS ; thus, treating together all operators in Σ , the new set of rules defines a function $\rho_S : \Sigma(TS \times BTS) \rightarrow BTS$. For example,

$$\rho_S(\parallel, P \mapsto f, Q \mapsto g) = \lambda a. \{P' \parallel Q : P' \in f(a)\} \cup \{P \parallel Q' : Q' \in g(a)\}.$$

It is easy to see that the ρ_S define a natural transformation $\rho : \Sigma(T \times BT) \rightarrow BT$, since the definition of ρ_S does not depend on any particular feature of S . In [2] it is shown that any set of rules in the GSOS format [9] gives rise to such a natural transformation, which is called “abstract GSOS” since it makes sense

⁴ Except for action prefix, to which we can add a premiss $P \mapsto f$, which is not actually used.

for any category of coalgebras, not just LTSs. It is shown in the same paper, using structural recursion, that ρ allows to define a B -coalgebra $\langle TS, \psi_S \rangle$ from $\langle S, \varphi \rangle$, the function ψ_S being the only one that makes the following diagram commute:

$$\begin{array}{ccccc}
 S & \xrightarrow{\eta_S} & TS & \xleftarrow{\alpha_S} & \Sigma TS \\
 \varphi \downarrow & & \downarrow \psi_S & & \downarrow \Sigma(1_{TS}, \psi_S) \\
 BS & \xrightarrow{B\eta_S} & BTS & \xleftarrow{\rho_S} & \Sigma(TS \times BTS).
 \end{array} \tag{1}$$

The definition already shows that η_S is a B -morphism, as required. Furthermore, the mapping of $\langle S, \varphi \rangle$ to $\langle TS, \psi_S \rangle$ extends to a functor by mapping any B -morphism f from $\langle S, \varphi \rangle$ to $\langle S', \varphi' \rangle$ to Tf , which can be shown to be a morphism from $\langle TS, \psi_S \rangle$ to $\langle TS', \psi_{S'} \rangle$. This applies in particular to $\iota_{TS} : T0 \rightarrow TS$, which results from the unique B -morphism from the initial B -coalgebra on 0 to $\langle S, \varphi \rangle$.

2.4 Bialgebraic Semantics Based on Finality

The standard way to associate “behaviours” with syntactic expressions is to structure the set Z of behaviours as a Σ -algebra or a B -coalgebra or both. In the first case, initiality of $T0$ allows to perform the association through the unique Σ -homomorphism $\iota_Z : T0 \rightarrow Z$. In the second case it is usually required that Z be a final coalgebra and the association is performed by the unique B -morphism $\beta_{T0} : T0 \rightarrow Z$, which as we have seen makes sense because $T0$ has also a coalgebraic structure. The Σ -homomorphism ι_Z is the initial or denotational semantics of $T0$ and the B -morphism β_{T0} is the final or operational semantics. In general one wishes to define both kinds of semantics and prove them equal. To give Z a transition structure $\zeta : Z \rightarrow BZ$ and to show that $\langle Z, \zeta \rangle$ is a final B -coalgebra is usually done directly; we shall write $\beta_S : S \rightarrow Z$ for the unique B -morphism from another B -coalgebra $\langle S, \varphi \rangle$. Assuming this has been done, the algebraic structure $\theta : \Sigma Z \rightarrow Z$ is defined by $\theta \hat{=} \beta_{TZ} \circ \alpha_Z \circ \Sigma\eta_Z$ as in the diagram:

$$\begin{array}{ccc}
 \Sigma TZ & \xleftarrow{\Sigma\eta_Z} & \Sigma Z \\
 \alpha_Z \downarrow & & \downarrow \theta \\
 TZ & \xrightarrow{\beta_{TZ}} & Z.
 \end{array} \tag{2}$$

Here, $\langle TZ, \alpha_Z \rangle$ is the free Σ -algebra generated by Z , with inclusion of generators $\eta_Z : Z \rightarrow TZ$, and $\beta_{TZ} : TZ \rightarrow Z$ results from the fact that $\langle Z, \zeta \rangle$ is a final B -coalgebra, since TZ inherits from Z a coalgebraic structure as shown in the last subsection. Now consider the diagram:

$$\begin{array}{ccc}
 & \xrightarrow{\iota_Z} & \\
 T0 & \xrightarrow{\iota_{TZ}} & TZ & \xrightarrow{\beta_{TZ}} & Z \\
 & \xrightarrow{\beta_{T0}} & & & \\
 & & & & \uparrow
 \end{array} \tag{3}$$

Since ι_{TZ} is also a B -morphism, as seen in the last subsection, we have $\beta_{TZ} \circ \iota_{TZ} = \beta_{T0}$, by finality. If we can prove that β_{TZ} is a Σ -homomorphism, this time we have $\beta_{TZ} \circ \iota_{TZ} = \iota_Z$, by initiality. In that case $\iota_Z = \beta_{T0}$ so the denotational and the operational semantics coincide. Now the fact that β_{TZ} is a Σ -homomorphism is automatic, requiring no further verification, provided that the structural operational rules are in some “well-behaved” format: in [1] this is shown for rules in the *tyft/tyxt* format; in the more abstract setting of [2], this is guaranteed by the abstract GSOS format.

We next extend this approach to behaviours that do not give rise to final coalgebras in the category of coalgebras of interest. When this happens, one possible solution is to consider another category (possibly a subcategory) in which the behaviours in question are a final object. This seems to be the approach followed by most authors, for example [14, 15, 10, 11, 12, 7]. Here we favour another approach, initiated in [8], which keeps the main category of interest but relaxes the requisite of finality to that of “quasi-finality,” as it will be called.

2.5 Quasi-Final Bialgebraic Semantics

We start by presenting a non-standard characterisation of finality and then show how it can be modified to account for quasi-finality. Assume given a category \mathbf{C} with identity endofunctor I . For any object C , let K_C be the constant endofunctor mapping any object to C and any morphism to the identity morphism 1_C .

Proposition 1. *An object Z of \mathbf{C} is final iff there is a natural transformation $\beta : I \rightarrow K_Z$ such that $\beta_Z = 1_Z$.*

Proof. The conditions in the proposition amount to say that (i) $\beta_{S'} \circ f = \beta_S$ for any morphism $f : S \rightarrow S'$, and (ii) $\beta_Z = 1_Z$; the situation is illustrated in the following diagram:

$$\begin{array}{ccc}
 \text{(i)} & S \xrightarrow{f} S' & \\
 & \searrow \beta_S \quad \swarrow \beta_{S'} & \\
 & Z & \\
 \text{(ii)} & Z & \\
 & \downarrow \beta_Z = 1_Z & \\
 & Z &
 \end{array}$$

Now if Z is final, the family of the unique morphisms $\beta_S : S \rightarrow Z$ clearly define a natural transformation $\beta : I \rightarrow K_Z$ with $\beta_Z = 1_Z$. Conversely, if such a natural transformation exists, each β_S is the unique morphism from S to Z ; indeed, given another morphism $f : S \rightarrow Z$, we have $\beta_Z \circ f = \beta_S$ because β is a natural transformation, hence $f = \beta_S$ since β_Z is the identity.

This characterisation of finality will now be generalised leading to the notion of quasi-finality. Quasi-final objects are defined in concrete categories only. So we assume that there is a base category \mathbf{B} and a faithful functor $U : \mathbf{C} \rightarrow \mathbf{B}$, known as the “forgetful” functor.

Definition 1. An object Z of \mathbf{C} is quasi-final iff there is a natural transformation $\beta : U \rightarrow UK_Z$ such that $\beta_Z = 1_{UZ}$. In detail, (i) $\beta_{S'} \circ Uf = \beta_S$ for any morphism $f : S \rightarrow S'$, and (ii) $\beta_Z = 1_{UZ}$:

$$(i) \quad \begin{array}{ccc} US & \xrightarrow{Uf} & US' \\ & \searrow \beta_S & \swarrow \beta_{S'} \\ & & UZ \end{array} \quad (ii) \quad \begin{array}{c} UZ \\ \downarrow \beta_Z = 1_{UZ} \\ UZ \end{array}$$

(Note that the β_S are morphisms in \mathbf{B} —just functions if \mathbf{B} is the category of sets—and f in condition (i) is a morphism in \mathbf{C} .)

A final object is of course quasi-final because from $\beta : I \rightarrow K_Z$ such that $\beta_Z = 1_Z$ we obtain $U\beta : U \rightarrow UK_Z$ such that $U\beta_Z = 1_{UZ}$. In the category of LTSs, the trace languages constitute a quasi-final LTS. Recall that a trace language over an alphabet A of actions is a subset L of A^* such that $\varepsilon \in L$ (ε is the null trace) and $x \in L$ whenever $xa \in L$, for all $x \in A^*$ and $a \in A$. The set \mathbb{T} of all trace languages can be made into a LTS by writing $L \xrightarrow{a} L'$ iff $a \in L$ and $L' = \{x : ax \in L\}$. For every LTS S the trace function $\text{Tr}_S : S \rightarrow \mathbb{T}$ assigns to every $s \in S$ the set $\text{Tr}_S(s)$ of all traces $a_1 \cdots a_n$ such that $s \xrightarrow{a_1} \cdots \xrightarrow{a_n} s'$ for some s' . If $f : S \rightarrow S'$ is a morphism of transition systems, any $s \in S$ and $f(s) \in S'$ have the same traces, that is, $\text{Tr}_{S'}(f(s)) = \text{Tr}_S(s)$. On the other hand, the set of traces of any L in the LTS \mathbb{T} is L itself, that is, $\text{Tr}_{\mathbb{T}}(L) = L$. These two properties show that \mathbb{T} is a quasi-final LTS. This example has been presented with more detail in [7, 8], along with other well-known behaviours from van Glabbeek's hierarchy [6] as well as quasi-final B -coalgebras extracted from the final sequence of the functor B .

Note that unlike final objects, quasi-final objects need not be unique up to isomorphism—there may be even infinitely many on the same underlying object of \mathbf{B} . For example, if \mathbf{B} has a final object 1 , any object Z in \mathbf{C} such that $UZ = 1$ is quasi-final. More concretely still, in the category of LTSs over A , any LTS with a single state and any number of transitions from the state to itself is quasi-final. This does not mean that quasi-final objects do not satisfy any uniqueness properties; in fact it is easy to find two categories in which quasi-final objects turn out to be final: one is a full sub-category of \mathbf{C} , the other a super-category of \mathbf{C} with the same objects and additional arrows.

By definition of quasi-finality, a morphism $f : S \rightarrow S'$ in \mathbf{C} “preserves behaviours” in the sense that $\beta_{S'} \circ Uf = \beta_S$; we now turn this property into a concept. For simplicity, from now on we identify a morphism f in \mathbf{C} with the morphism Uf in \mathbf{B} , as is customary when dealing with forgetful functors. For any objects S, S' in \mathbf{C} , a morphism $f : US \rightarrow US'$ in \mathbf{B} is called a β -map if $\beta_{S'} \circ f = \beta_S$. Morphisms f in \mathbf{C} , with the identification $Uf = f$, are β -maps. Any $\beta_S : S \rightarrow Z$ is also a β -map since $\beta_Z \circ \beta_S = 1_Z \circ \beta_S = \beta_S$. Furthermore, β_S is the only β -map from S to Z : another β -map $f : S \rightarrow Z$ satisfies $\beta_S = \beta_Z \circ f = f$. Thus, Z is final in the category \mathbf{C}/β that has the same objects as \mathbf{C} and β -maps as morphisms.

Next consider the full sub-category \mathbf{D} of \mathbf{C} whose objects are those S for which β_S is actually a morphism in \mathbf{C} ; we show that Z is final in \mathbf{D} (note that Z is in \mathbf{D} because β_Z is the identity morphism). For any S in \mathbf{D} , if $f : S \rightarrow Z$ is another morphism in \mathbf{D} , then f is a β -map, hence, as we saw, f must be equal to β_S . For this notion to be useful, however, we should be able to obtain the behaviours of objects not in \mathbf{D} in terms of the behaviours of those in \mathbf{D} . In [7] we achieved this through a functor $T : \mathbf{C} \rightarrow \mathbf{D}$ and a natural transformation $\tau : U \rightarrow UT$ such that $\beta_S = \beta_{TS} \circ \tau_S$ for every S in \mathbf{C} , that is, every τ_S is a β -map. Note that an extreme (and uninteresting!) possibility is to let \mathbf{D} be formed by Z alone together with its identity morphism, T be the constant functor with value Z and τ be β . We shall not pursue this line here, but see the examples in [7].

We apply these notions to the case where \mathbf{C} is the category \mathbf{Coalg}_B of B -coalgebras, \mathbf{B} is the category \mathbf{Sets} of sets and functions, and the forgetful functor maps a coalgebra to its underlying set and a B -morphism to itself as a function. Given again the signature Σ and the set $T0$ of Σ -terms, the operational is defined as before as $\beta_{T0} : T0 \rightarrow Z$, except that now $\langle Z, \zeta \rangle$ is a quasi-final coalgebra with respect to a behaviour β . The algebraic structure $\theta : \Sigma Z \rightarrow Z$ is again defined by (2), which allows to define the denotational semantics by the unique Σ -homomorphism $\iota_Z : T0 \rightarrow Z$. Once again, the equality $\beta_{T0} = \iota_Z$ follows if $\beta_{TZ} : TZ \rightarrow Z$ is a Σ -homomorphism. Referring to (3), we have $\iota_Z = \beta_{TZ} \circ \iota_{TZ}$ as before, but the equality $\beta_{T0} = \beta_{TZ} \circ \iota_{TZ}$ now follows from the fact that ι_{TZ} is a B -morphism, hence a β -map.

That β_{TZ} is a Σ -homomorphism is no longer a consequence of the fact that the transition rules are in some well-behaved format, as is the case for finality. At the time of writing we still do not know any set of general conditions that automatically guarantee that β_{TZ} is a Σ -homomorphism, so we have to make the verification directly in each case. We must verify then that the following diagram commutes:

$$\begin{array}{ccc} \Sigma TZ & \xrightarrow{\Sigma \beta_{TZ}} & \Sigma Z \\ \alpha_Z \downarrow & & \downarrow \theta \\ TZ & \xrightarrow{\beta_{TZ}} & Z. \end{array}$$

Let us illustrate what is required by considering, without loss of generality, a binary operator \otimes written in infix notation:

$$\begin{array}{ccc} \langle \otimes, t, u \rangle & \xrightarrow{\Sigma \beta_{TZ}} & \langle \otimes, \beta_{TZ}(t), \beta_{TZ}(u) \rangle \\ \alpha_Z \downarrow & & \downarrow \theta \\ t \otimes u & \xrightarrow{\beta_{TZ}} & \beta_{TZ}(\beta_{TZ}(t) \otimes \beta_{TZ}(u)) \\ & & = \\ & & \beta_{TZ}(t \otimes u). \end{array}$$

Thus, we must have

$$\beta_{TZ}(t \otimes u) = \beta_{TZ}(\beta_{TZ}(t) \otimes \beta_{TZ}(u)) \quad (4)$$

for all $t, u \in TZ$. To prove (4) we use a simple property of coalgebras: if $\langle S, \varphi \rangle$ is a B -coalgebra, then $\langle BS, B\varphi \rangle$ is also a B -coalgebra and $\varphi : S \rightarrow BS$ is a B -morphism. Thus, in particular, φ is a β -map, so $\beta_S = \beta_{BS} \circ \varphi$. In the case at hand we have $\beta_{TZ} = \beta_{BTZ} \circ \psi_Z$, with $\psi_Z : TZ \rightarrow BTZ$ defined as in (1). With this result, (4) may be rewritten as

$$\beta_{BTZ}(\psi_Z(t \otimes u)) = \beta_{BTZ}(\psi_Z(\beta_{TZ}(t) \otimes \beta_{TZ}(u))). \quad (5)$$

The advantage of (5) over (4) is that the behaviour of expressions has been replaced by the behaviour of their “next steps”, whose structure is determined by the operational rules of the language and allows a form of inductive reasoning.

Let us illustrate our approach with the trace semantics and the interleaving operator (for the other operators in the fragment of CSP we have been considering the verification is immediate). As far as notation is concerned, \mathbb{T} is the set of trace languages and β is the family Tr of trace functions, so the appropriate instance of (4) is

$$\text{Tr}(P \parallel Q) = \text{Tr}(\text{Tr}(P) \parallel \text{Tr}(Q)),$$

where we abbreviated $\text{Tr}_{\mathbb{T}}$ to Tr for readability; we prove by induction on n that both sides have the same traces of length less than or equal to n . This is immediate for $n = 0$, since both sides contain ε , the only trace of length zero. Now let us assume the result for n . We now that, in general, $\text{Tr}(P)$ is the union of $\{\varepsilon\}$ with the $a \cdot \text{Tr}(P') = \{ax : x \in \text{Tr}(P')\}$ such that $P \xrightarrow{a} P'$, so we can write

$$\text{Tr}(P \parallel Q) = \{\varepsilon\} \cup \bigcup_{a \in A} a \cdot \left(\bigcup_{P \xrightarrow{a} P'} \text{Tr}(P' \parallel Q) \cup \bigcup_{Q \xrightarrow{a} Q'} \text{Tr}(P \parallel Q') \right),$$

$$\text{Tr}(\text{Tr}(P) \parallel \text{Tr}(Q)) =$$

$$\{\varepsilon\} \cup \bigcup_{a \in A} a \cdot \left(\bigcup_{\text{Tr}(P) \xrightarrow{a} L} \text{Tr}(L \parallel \text{Tr}(Q)) \cup \bigcup_{\text{Tr}(Q) \xrightarrow{a} M} \text{Tr}(\text{Tr}(P) \parallel M) \right).$$

(The equality of the two right-end sides of these equations is nothing but the instance of (5) for this case.) Note that $P \xrightarrow{a}$ iff $\text{Tr}(P) \xrightarrow{a}$. When this is the case, there is a unique L such that $\text{Tr}(P) \xrightarrow{a} L$, namely $L = \bigcup_{P \xrightarrow{a} P'} \text{Tr}(P')$, so the union $\bigcup_{\text{Tr}(P) \xrightarrow{a} L} \text{Tr}(L \parallel \text{Tr}(Q))$ reduces to $\text{Tr}(\bigcup_{P \xrightarrow{a} P'} \text{Tr}(P') \parallel \text{Tr}(Q))$. It is not difficult to see that the last expression is equal to $\bigcup_{P \xrightarrow{a} P'} \text{Tr}(\text{Tr}(P') \parallel \text{Tr}(Q))$, so we are ready for the inductive step. By the induction hypothesis, $\text{Tr}(P' \parallel Q)$ and $\text{Tr}(\text{Tr}(P') \parallel \text{Tr}(Q))$ have the same traces of length at most n , so the same happens to $\bigcup_{P \xrightarrow{a} P'} \text{Tr}(P' \parallel Q)$ and $\bigcup_{P \xrightarrow{a} P'} \text{Tr}(\text{Tr}(P') \parallel \text{Tr}(Q)) = \bigcup_{\text{Tr}(P) \xrightarrow{a} L} \text{Tr}(L \parallel \text{Tr}(Q))$. A symmetric reasoning applies to the two other unions in the previous equations. We conclude that $\text{Tr}(P \parallel Q)$ and $\text{Tr}(\text{Tr}(P) \parallel \text{Tr}(Q))$ have the same traces of length at most $n + 1$.

In the next section we apply this technique to the failure semantics of CSP.

3 Bialgebraic Quasi-Failure Semantics of CSP

3.1 Transition Systems with Internal Transitions

Let $A \neq \emptyset$ be a set of *actions*; this set will be fixed throughout this section. A *transition system with labels in A and internal actions* is just a LTS with labels in $A + 1$, where 1 is a singleton. We write $A + 1 = A \cup \{\tau\}$ with $\tau \notin A$, so transitions $s \xrightarrow{a} t$ have $a \in A$ or $a = \tau$. When viewed as coalgebras, such transition systems are pairs $\mathbf{S} = \langle S, \varphi \rangle$ with $\varphi : S \rightarrow \mathcal{P}(S)^{A+1}$; their morphisms are the morphisms as transition systems over $A + 1$. The category of transition systems with internal actions will be denoted \mathbf{LTR}_τ ; the category of transition systems without internal transitions will be identified with the full subcategory of \mathbf{LTR}_τ formed by the systems $\mathbf{S} = \langle S, \varphi \rangle$ such that $\varphi(s)(\tau) = \emptyset$ for all $s \in S$. In the sequel, by “transition system” or LTS we shall always mean “labelled transition system with internal actions” unless the contrary is explicitly stated. The forgetful functor $U : \mathbf{LTR}_\tau \rightarrow \mathbf{Sets}$ sends $\mathbf{S} = \langle S, \varphi \rangle$ to S and any morphism to itself as a function.

For any $a \in A$, define \xrightarrow{a} as $(\xrightarrow{\tau})^* \xrightarrow{a} (\xrightarrow{\tau})^*$, where $(\xrightarrow{\tau})^*$ is the reflexive-transitive closure of $\xrightarrow{\tau}$; for arbitrary strings over A , define $\xrightarrow{\varepsilon}$ as $(\xrightarrow{\tau})^*$ and \xrightarrow{xy} as the relational composition $\xrightarrow{x} \xrightarrow{y}$; finally, define $\xrightarrow{\tau}$ as $\xrightarrow{\tau} (\xrightarrow{\tau})^*$, the transitive closure of $\xrightarrow{\tau}$. The strings x such that $s \xrightarrow{x} t$ for some t are the *traces* of s ; we put $\text{Tr}(s) = \{x : \exists t, s \xrightarrow{x} t\}$. The set $\text{Tr}(s)$ is nonempty and prefix-closed; this amounts to say that $\varepsilon \in \text{Tr}(s)$ and whenever $xy \in \text{Tr}(s)$, then $x \in \text{Tr}(s)$. It is easy to see that morphisms preserve traces, in the sense that any morphism $f : \mathbf{S}_1 \rightarrow \mathbf{S}_2$ satisfies $\text{Tr}_{\mathbf{S}_1}(s) = \text{Tr}_{\mathbf{S}_2}(f(s))$ for every s in \mathbf{S}_1 (any path in \mathbf{S}_1 starting in s has a path in \mathbf{S}_2 starting in $f(s)$ with exactly the same labels, and vice-versa).

The relations \xrightarrow{a} ($a \in A$) and $\xrightarrow{\tau}$ define a transition system $\mathbf{S}^* = \langle S, \varphi^* \rangle$. For this system, we may go from \Rightarrow to a relation \Rightarrow as we did go from \rightarrow to \Rightarrow , but it turns out that \Rightarrow coincides with \Rightarrow , as it is easy to see. Indeed, first note that $(\xrightarrow{\tau})^* = (\xrightarrow{\tau} (\xrightarrow{\tau})^*)^* = (\xrightarrow{\tau})^*$; now \xrightarrow{a} is $(\xrightarrow{\tau})^* \xrightarrow{a} (\xrightarrow{\tau})^*$, that is, $(\xrightarrow{\tau})^* (\xrightarrow{\tau})^* \xrightarrow{a} (\xrightarrow{\tau})^* (\xrightarrow{\tau})^*$, which is \xrightarrow{a} ; in the same vein, $\xrightarrow{\varepsilon}$ is $(\xrightarrow{\tau})^*$, so coincides with $\xrightarrow{\varepsilon}$; finally, $\xrightarrow{\tau}$ is $\xrightarrow{\tau} (\xrightarrow{\tau})^*$, that is, $\xrightarrow{\tau} (\xrightarrow{\tau})^* (\xrightarrow{\tau})^*$, which is $\xrightarrow{\tau}$. This shows, in particular, that $(\mathbf{S}^*)^* = \mathbf{S}^*$. As a consequence, all notions defined in \mathbf{S} using \Rightarrow coincide with the same notions in \mathbf{S}^* using \Rightarrow again. For example, any $s \in S$ has the same traces in \mathbf{S} and in \mathbf{S}^* ; the same can be said of initials, refusals and failures, to be introduced below.

It is easy to see that a morphism $f : \mathbf{S}_1 \rightarrow \mathbf{S}_2$ of transition systems, as a function $f : S_1 \rightarrow S_2$, is also a morphism $f : \mathbf{S}_1^* \rightarrow \mathbf{S}_2^*$ (but the converse is not true). This defines an endofunctor $(-)^*$ on \mathbf{LTR}_τ where $f^* = f$. The identity function on S is not in general a morphism $\mathbf{S} \rightarrow \mathbf{S}^*$, but is the \mathbf{S} -component of a natural transformation $U \rightarrow U \circ (-)^*$. Note, however, that 1_S is a morphism $\mathbf{S}^* \rightarrow (\mathbf{S}^*)^*$, since $(\mathbf{S}^*)^* = \mathbf{S}^*$. A function $S_1 \rightarrow S_2$ will be called a *weak morphism* if it is a morphism $\mathbf{S}_1^* \rightarrow \mathbf{S}_2^*$; in particular, 1_S is a weak morphism $\mathbf{S} \rightarrow \mathbf{S}^*$. We

noticed that every $s \in S$ has the same traces in S and in S^* ; more generally, if $f : S_1 \rightarrow S_2$ is a weak morphism, then $\text{Tr}(s) = \text{Tr}(f(s))$ for every $s \in S_1$.⁵

If $\xrightarrow{\tau} \xrightarrow{\tau} \subseteq \xrightarrow{\tau}$ and $\xrightarrow{a} \xrightarrow{\tau} \cup \xrightarrow{\tau} \xrightarrow{a} \subseteq \xrightarrow{a}$ for all $a \in A$, we say the transition system is *transitive*. An equivalent condition is that $\xrightarrow{\tau}$ and \xrightarrow{a} ($a \in A$) coincide with $\xrightarrow{\tau}$ and \xrightarrow{a} , respectively. Thus, a transition system S is transitive iff $S = S^*$; in particular, S^* is transitive. For a transitive system we shall also write \xrightarrow{x} instead of \xrightarrow{a} when $x \in A^*$.

3.2 Failures of Transition Systems

Let $S = \langle S, \varphi \rangle$ be a transition system and $s \in S$. The set of *continuations* of s after $x \in A^*$ is $C_s(x) = \{a \in A : \exists t, s \xrightarrow{xa} t\}$; the continuations of s after the null trace ε are the *initials* of s , and we put $I(s) = C_s(\varepsilon) = \{a \in A : \exists t, s \xrightarrow{a} t\}$; the set of *failures* of s is $Fl(s) = \{(x, X) \in A^* \times \mathcal{P}(A) : \exists t, s \xrightarrow{x} t \text{ and } I(t) \cap X = \emptyset\}$; a *refusal* of s is a set $X \subseteq A$ such that (ε, X) is a failure of s ; the set of refusals of s is written $Rf(s)$. Clearly, (x, \emptyset) is a failure of s iff $s \xrightarrow{x} t$ for some t , so the traces are in bijective correspondence with the failures with empty refusal. Note that in [17] a failure (x, X) has X a finite subset of A ; for simplicity we shall not make that requirement here. When there is danger of confusion we write $C_{S,s}$, I_S , Fl_S and Rf_S instead of their uns subscripted versions, but we will try to avoid subscripts as much as possible for readability.

Note that s has the same continuations, initials, failures and refusals with respect to S and S^* . As we did for traces, the previous statement generalizes to arbitrary weak morphisms $f : S_1 \rightarrow S_2$. Thus, if $s \in S_1$, we have $C_s(x) = C_{f(s)}(x)$, because s and $f(s)$ have the same traces, so that s has trace xa iff $f(s)$ has trace xa ; in particular, $I(s) = I(f(s))$. The next lemma takes care of failures and refusals.

Lemma 1. *If $f : S_1 \rightarrow S_2$ is a weak morphism and $s \in S_1$, then $Fl(s) = Fl(f(s))$. In particular, $Rf(s) = Rf(f(s))$.*

Proof. If $(x, X) \in Fl(s)$, then $s \xrightarrow{x} t$ and $I(t) \cap X = \emptyset$ for some t . As f is a weak morphism, $f(s) \xrightarrow{x} f(t)$ and $I(f(t)) \cap X = I(t) \cap X = \emptyset$. We conclude that $(x, X) \in Fl(f(s))$. Conversely, suppose that $(x, X) \in Fl(f(s))$, that is, $f(s) \xrightarrow{x} t'$ and $I(t') \cap X = \emptyset$ for some t' . Consider first the case where $x = \varepsilon$. If $t' = f(s)$, then $I(s) \cap X = I(f(s)) \cap X = \emptyset$, so $(\varepsilon, X) \in Fl(s)$. If $t' \neq f(s)$, then in fact $f(s) \xrightarrow{\tau} t'$; as f is a weak morphism, there is t such that $s \xrightarrow{\tau} t$ and $f(t) = t'$. We have $I(t) \cap X = I(f(t)) \cap X = \emptyset$, so once again $(\varepsilon, X) \in Fl(s)$. Let us next consider the case where x is not empty, say $x = a_1 \cdots a_n$ with $a_1, \dots, a_n \in A$ and $n > 0$. Any sequence $s \xrightarrow{a_1} s_1 \cdots \xrightarrow{a_n} s_n$ in S_1 gives a sequence $f(s) \xrightarrow{a_1} f(s_1) \cdots \xrightarrow{a_n} f(s_n)$ in S_2 ; since s_n and $f(s_n)$ have the same initials, this shows that $Fl(s) \subseteq Fl(f(s))$. Conversely, for any sequence $f(s) \xrightarrow{a_1} s'_1 \cdots \xrightarrow{a_n} s'_n$ in

⁵ Adding subscripts to the trace functions to disambiguate, we can write $\text{Tr}_{S_1}(s) = \text{Tr}_{S_1^*}(s) = \text{Tr}_{S_2^*}(f(s)) = \text{Tr}_{S_2}(f(s))$, where the middle equality is due to the fact that f is a morphism $S_1^* \rightarrow S_2^*$ and morphisms preserve traces.

S_2 there is a sequence $s \xrightarrow{a_1} s_1 \cdots \xrightarrow{a_n} s_n$ in S_1 such that $f(s_i) = s'_i$ for all $i = 1, \dots, n$; again, s_n and s'_n have the same initials, and we conclude that $Fl(f(s)) \subseteq Fl(s)$.

A *failure-set* over A is any set $P \subseteq A^* \times \mathcal{P}(A)$ such that the following conditions hold:

- F1** $(\varepsilon, \emptyset) \in P$.
- F2** $(xy, \emptyset) \in P \Rightarrow (x, \emptyset) \in P$.
- F3** $(x, X) \in P \wedge Y \subseteq X \Rightarrow (x, Y) \in P$.
- F4** $(x, X) \in P \wedge \forall a \in Y, (xa, \emptyset) \notin P \Rightarrow (x, X \cup Y) \in P$.

Let \mathcal{F} be the set of all failure sets. We turn \mathcal{F} into a transition system $F = \langle \mathcal{F}, \zeta_{Fl} \rangle$ by defining the transitions associated with ζ_{Fl} as follows. Let P and Q be failure-sets; we write

$$\begin{aligned} P \xrightarrow{\tau} Q & \text{ iff } Q \subsetneq P; \\ P \xrightarrow{a} Q & \text{ iff } \forall (x, X) \in Q, (ax, X) \in P. \end{aligned}$$

(Here, $Q \subsetneq P$ means that Q is a proper subset of P .)

Lemma 2. *The transition system $F = \langle \mathcal{F}, \zeta_{Fl} \rangle$ is transitive.*

Proof. This is straightforward. If $P \xrightarrow{\tau} Q \xrightarrow{\tau} R$, then $R \subsetneq Q \subsetneq P$, hence $P \xrightarrow{\tau} R$. If $P \xrightarrow{a} Q \xrightarrow{\tau} R$, then $(ax, X) \in P$ for all $(x, X) \in Q$, hence for all $(x, X) \in R$, so $P \xrightarrow{a} R$. Finally, suppose $P \xrightarrow{\tau} Q \xrightarrow{a} R$; for all $(x, X) \in R$, $(ax, X) \in Q$, hence $(ax, X) \in P$; it follows that $P \xrightarrow{a} R$.

Our immediate goal is to show how the sets $\text{Tr}(P)$, $C_P(x)$, $I(P)$, $Fl(P)$ and $Rf(P)$, where P is a failure-set, can be defined in terms of the set P itself rather than the transitions from P in F . For this we need to establish some auxiliary results first. We start with a result that shows that whenever there is a transition $P \xrightarrow{a} Q$, there is a largest such Q , so that $Q \xrightarrow{\varepsilon} R$ for any R such that $P \xrightarrow{a} R$.

Lemma 3. *If $(a, \emptyset) \in P$, then $Q = \{(x, X) : (ax, X) \in P\}$ is in \mathcal{F} and $P \xrightarrow{a} Q$. For any $R \in \mathcal{F}$ such that $P \xrightarrow{a} R$, we have $Q \xrightarrow{\varepsilon} R$.*

Proof. The condition $(a, \emptyset) \in P$ is needed to show that $(\varepsilon, \emptyset) \in Q$, which is **F1**. Conditions **F2** and **F3** are easy. Let us check **F4**. Suppose $(x, X) \in Q$ and $(xc, \emptyset) \notin Q$ for every $c \in Y$. Then $(ax, X) \in P$ and $(axc, \emptyset) \notin P$ for every $c \in Y$, by definition of Q . Since P satisfies **F4**, $(ax, X \cup Y) \in P$. Again by definition of Q , $(x, X \cup Y) \in Q$, as required. The remaining statements are immediate consequences of the definition of the transition relation \xrightarrow{a} in F .

The next lemma generalizes both the definition of \xrightarrow{a} and the previous lemma to arbitrary strings x .

Lemma 4. *Let $P \in \mathcal{F}$ and $x \in A^*$.*

1. For any $Q \in \mathcal{F}$, $P \xrightarrow{x} Q$ iff for every $(y, X) \in Q$, $(xy, X) \in P$.
2. If $(x, \emptyset) \in P$, then $Q = \{(y, X) : (xy, X) \in P\}$ is in \mathcal{F} and $P \xrightarrow{x} Q$. For any $R \in \mathcal{F}$ such that $P \xrightarrow{x} R$, we have $Q \xrightarrow{\varepsilon} R$.

Proof. 1. The result is proved by induction on the length of x . For the null string ε , since $\xrightarrow{\varepsilon}$ is the reflexive closure of $\xrightarrow{\tau}$, we have $P \xrightarrow{\varepsilon} Q$ iff $P = Q$ or $P \xrightarrow{\tau} Q$, iff $Q \subseteq P$, iff for all $(y, X) \in Q$, $(y, X) \in P$. For a string ax , assume first $P \xrightarrow{ax} Q$, so that $P \xrightarrow{a} R \xrightarrow{x} Q$ for some $R \in \mathcal{F}$. If $(y, X) \in Q$, then, by induction hypothesis, $(xy, X) \in R$, hence $(axy, X) \in P$, by definition of \xrightarrow{a} . Conversely, assume $(axy, X) \in P$ for all $(y, X) \in Q$. Letting $R = \{(z, X) : (az, X) \in P\}$, we know that $R \in \mathcal{F}$ and $P \xrightarrow{a} R$; we show that $R \xrightarrow{x} Q$, which allows to conclude that $P \xrightarrow{ax} Q$, as required. So take $(y, X) \in Q$; we have $(axy, X) \in P$, by hypothesis, hence $(xy, X) \in R$, by definition of R . Thus, $(xy, X) \in R$ for all $(y, X) \in Q$, so by induction hypothesis, $R \xrightarrow{x} Q$, as desired.

2. We also use induction on the length of x . For the empty string, the statement just says that when $Q = P$, then $Q \in \mathcal{F}$ and $P \xrightarrow{\varepsilon} Q$, which is immediate. For a string ax we can write $Q = \{(y, X) : (xy, X) \in R\}$ where $R = \{(z, X) : (az, X) \in P\}$. We have $P \xrightarrow{a} R$ and, by induction hypothesis, $Q \in \mathcal{F}$ and $R \xrightarrow{x} Q$. It follows that $P \xrightarrow{ax} Q$, as required. The second statement is now immediate, because $P \xrightarrow{x} R$ implies $R \subseteq Q$, hence $Q \xrightarrow{\varepsilon} R$. This ends the proof.

Lemma 5. *Let P be a failure-set. In $\mathbf{F} = \langle \mathcal{F}, \zeta_{\mathbf{F1}} \rangle$ the following equalities hold:*

1. $\text{Tr}(P) = \{x \in A^* : (x, \emptyset) \in P\}$.
2. $C_P(x) = \{a \in A : (xa, \emptyset) \in P\}$.
3. $I(P) = \{a \in A : (a, \emptyset) \in P\}$.

Proof. 1. If $P \xrightarrow{x} Q$, then, since $(\varepsilon, \emptyset) \in Q$ and by the first statement of Lemma 4, $(x, \emptyset) \in P$. Conversely, if $(x, \emptyset) \in P$, the second statement of Lemma 4 immediately implies that $x \in \text{Tr}(P)$.

2. To say that $a \in C_P(x)$ is equivalent, by definition, to say that xa is a trace of P , which by the previous result is equivalent to $(xa, \emptyset) \in P$.

3. This is because $I(P) = C_P(\varepsilon)$.

Lemma 6. *If $P \in \mathcal{F}$ and $(\varepsilon, X) \in P$, then*

$$Q = \{(\varepsilon, Y) : (\varepsilon, X \cup Y) \in P\} \cup \{(ax, Y) \in P : a \notin X\}$$

is in \mathcal{F} , $P \xrightarrow{\varepsilon} Q$ and $I(Q) \cap X = \emptyset$. For any $R \in \mathcal{F}$ such that $P \xrightarrow{\varepsilon} R$ and $I(R) \cap X = \emptyset$, we have $Q \xrightarrow{\varepsilon} R$.

Proof. We first show that Q satisfies the axioms **F1** through **F4**. For **F1** note that $(\varepsilon, \emptyset) \in Q$ because $(\varepsilon, X) \in P$. For **F2** assume $(yz, \emptyset) \in Q$, to conclude that $(y, \emptyset) \in Q$; if y is ε , it was already proved that $(\varepsilon, \emptyset) \in Q$; otherwise, $y = ax$, $(axz, \emptyset) \in P$ and $a \notin X$; by **F2** applied to P , $(ax, \emptyset) \in P$, hence $(ax, \emptyset) \in Q$. For **F3** let $(y, Y) \in Q$ and $Z \subseteq Y$; if $y = \varepsilon$, then $(\varepsilon, X \cup Y) \in P$, in which

case $(\varepsilon, X \cup Z) \in P$, because P satisfies **F3**, so $(\varepsilon, Z) \in Q$; if $y = ax$, then $(ax, Y) \in P$ and $a \notin X$, which implies $(ax, Z) \in P$, because P satisfies **F3**, so $(ax, Z) \in Q$. Finally, let us consider **F4**; we must show that if $(y, Y) \in Q$ and $\forall c \in W, (yc, \emptyset) \notin Q$, then $(y, Y \cup W) \in Q$. If y is ε , then $(\varepsilon, X \cup Y) \in P$; let $W_1 = \{c \in Y : (c, \emptyset) \notin P\}$ and $W_2 = \{c \in Y : (c, \emptyset) \in P\}$, then $(\varepsilon, X \cup Y \cup W_1) \in P$, since P satisfies **F4**, so $(\varepsilon, Y \cup W_1) \in Q$. We have $W_2 \subseteq X$, since if $(c, \emptyset) \in P$ and $(c, \emptyset) \notin Q$, then $c \in X$, hence $(\varepsilon, X \cup Y \cup W_1 \cup W_2) \in P$ and $(\varepsilon, Y \cup W) \in Q$; finally, if y is ax , then $a \notin X$, $(ax, Y) \in P$ and $(axc, \emptyset) \notin P$, so $(ax, Y \cup \{c\}) \in P$ by **F4**, therefore $(ax, Y \cup \{c\}) \in Q$.

This shows $Q \in \mathcal{F}$. By construction, $Q \subseteq P$, hence $P \xrightarrow{\varepsilon} Q$; also by construction, $I(Q) \cap X = \emptyset$. Now consider R in the conditions of the lemma. If $(\varepsilon, Y) \in R$, then, since $(c, \emptyset) \notin R$ for every $c \in X$, because $I(R) \cap X = \emptyset$, we conclude that $(\varepsilon, X \cup Y) \in R$ by **F4**; but then $(\varepsilon, X \cup Y) \in P$, so $(\varepsilon, Y) \in Q$. If $(ax, Y) \in R$, then $(ax, Y) \in P$ and $a \notin X$, because $I(R) \cap X = \emptyset$, hence $(ax, Y) \in Q$. This ends the proof.

Lemma 7. *If $P \in \mathcal{F}$ then $Q = \{(x, X) \in P : \forall a \in X, (xa, \emptyset) \notin P\}$ is in \mathcal{F} and $P \xrightarrow{\varepsilon} Q \not\rightarrow$.*

Proof. First note that $(x, \emptyset) \in Q$ iff $(x, \emptyset) \in P$. Axioms **F1** through **F4** are easy to check. Since $Q \subseteq P$ then $P \xrightarrow{\varepsilon} Q$. For the last conditions, let $R \subseteq Q$ be a failure set, and prove, by induction on the length of failures, that $R = Q$; for the empty string let $(\varepsilon, X) \in Q$, since $R \subseteq Q \subseteq P$, $\forall a \in X, (a, \emptyset) \notin R$; by **F1** $(\varepsilon, \emptyset) \in R$ and by **F4** $(\varepsilon, X) \in R$. Assume that for all failures of length n , $(x, X) \in Q \Rightarrow (x, X) \in R$ and take a failure $(xa, X) \in Q$ of length $n + 1$, that is, $a \in A$ and x has length n ; by **F3** and **F2**, $(x, \emptyset) \in Q$ and, by induction hypothesis, $(x, \emptyset) \in R$; by **F3** $(xa, \emptyset) \in Q \subseteq P$ and by definition of Q , $(x, \{a\}) \notin Q$ then, $(xa, \emptyset) \in R$, because if $(xa, \emptyset) \notin R$, by **F3**, $(x, \{a\}) \in R \subseteq Q$; by definition of Q , $\forall b \in X, (xab, \emptyset) \notin P$. Since $R \subseteq Q \subseteq P$, $\forall b \in X, (xab, \emptyset) \notin R$ and by **F4** $(xa, X) \in R$.

Lemma 8. *Let P be a failure-set. In $\mathbf{F} = \langle \mathcal{F}, \zeta_{Fl} \rangle$ the following equalities hold:*

1. $Rf(P) = \{X \subseteq A : (\varepsilon, X) \in P\}$.
2. $Fl(P) = P$.

Proof. 1. If $X \in Rf(P)$, there is Q such that $P \xrightarrow{\varepsilon} Q$ and $I(Q) \cap X = \emptyset$. Thus, $(a, \emptyset) \notin Q$ for every $a \in X$. Starting from $(\varepsilon, \emptyset) \in Q$ we conclude by **F4** that $(\varepsilon, X) \in Q$; as $Q \subseteq P$, $(\varepsilon, X) \in P$. Conversely, if $(\varepsilon, X) \in P$, there is Q such that $P \xrightarrow{\varepsilon} Q$ and $I(Q) \cap X = \emptyset$, by Lemma 6, so $X \in Rf(P)$.

2. Let $(x, X) \in Fl(P)$. There is Q such that $P \xrightarrow{x} Q$ and $I(Q) \cap X = \emptyset$. But then $X \in Rf(Q)$, so $(\varepsilon, X) \in Q$. By the first statement of Lemma 4, $(x, X) \in P$. Conversely, let $(x, X) \in P$. By **F3**, $(x, \emptyset) \in P$, so by the second statement of Lemma 4, there is Q such that $P \xrightarrow{x} Q$ and $(\varepsilon, X) \in Q$. We have $X \in Rf(Q)$, so there is R such that $Q \xrightarrow{\varepsilon} R$ and $I(R) \cap X = \emptyset$. Together with $P \xrightarrow{x} Q$, this implies that $(x, X) \in Fl(P)$.

Lemma 1 and Lemma 8 imply that $\mathbf{F} = \langle \mathcal{F}, \zeta_{Fl} \rangle$ is quasi-final with respect to behaviour Fl .

3.3 Some Auxiliary Notions and Notation

In the sequel we need the following result:

Lemma 9. *If $(P_i)_{i \in I}$ is a nonempty family of failure sets, $\bigcup_{i \in I} P_i$ is a failure set.*

Proof. Conditions **F1** through **F3** are immediate. For **F4**, assume $(x, X) \in \bigcup_{i \in I} P_i$ and $(xa, \emptyset) \notin \bigcup_{i \in I} P_i$ for all $a \in Y$. Then $(x, X) \in P_j$ for some $j \in I$ and $(xa, \emptyset) \notin P_k$ for all $a \in A$ and $k \in I$. In particular, $(xa, \emptyset) \notin P_j$ for all $a \in A$, hence $(x, X \cup Y) \in P_j \subseteq \bigcup_{i \in I} P_i$.

Given $a \in A$ and $F \in \mathcal{F}$, we put

$$\begin{aligned} a \cdot F &= \{(ax, X) : (x, X) \in F\}, \\ \partial_a(F) &= \{(x, X) : (ax, X) \in F\}. \end{aligned}$$

Clearly, $\partial_a(a \cdot F) = F$, and $a \cdot \partial_a(F)$ is the set of failures in F whose traces start with a .

For an arbitrary transition system $S = \langle S, \varphi \rangle$ and any $s \in S$, we shall use the fact that

$$Fl(s) = N(s) \cup \bigcup_{a \in A} a \cdot \bigcup_{s \xrightarrow{a} s'} Fl(s') \quad (6)$$

(note the use of the transitions \xrightarrow{a} rather than \xrightarrow{a}), where

$$N(s) = \{(\varepsilon, X) : \exists s' \forall a \in X, s \xrightarrow{\varepsilon} s' \not\xrightarrow{a}\}. \quad (7)$$

As a consequence, for all $a \in A$,

$$\partial_a(Fl(s)) = \bigcup_{s \xrightarrow{a} s'} Fl(s'). \quad (8)$$

It is useful to extend the definition of ∂ to any $x \in A^*$ by $\partial_x(P) = \{(y, X) : (xy, X) \in P\}$; this defines a function $\partial_x : \mathcal{F} \rightarrow \mathcal{F} \cup \{\emptyset\}$ that coincides with ∂_a when x is a . Equivalently, $\partial_\varepsilon(P) = P$ for any P and $\partial_{ax} = \partial_x \circ \partial_a$. By Lemma 4, $\partial_x(P) \in \mathcal{F}$ if $(x, \emptyset) \in P$; in that case, $P \xrightarrow{x} \partial_x(P)$ and $\partial_x(P) \xrightarrow{\varepsilon} P'$ whenever $P \xrightarrow{x} P'$. A simple induction on the length of x shows that (8) generalizes to

$$\partial_x(Fl(s)) = \bigcup_{s \xrightarrow{x} s'} Fl(s'). \quad (9)$$

Remark 1. For a transitive system like **F**, the relation \Rightarrow is equal to \rightarrow , but for clarity we still use \Rightarrow whenever appropriate.

3.4 Failures of Transition Systems with termination

With the extended alphabet $A^\surd = A \cup \{\surd\}$ ($\surd \notin A + 1$ represents the termination action) we need to introduce some complements to previous definitions and results.

A *transition system with labels in A , internal actions and termination* is just a LTS with labels in $A^{\tau\surd} = A^\surd + 1 = A^\surd \cup \{\tau\}$, such that, if $s \xrightarrow{\surd} t$ then $t \not\xrightarrow{a}$, for all $a \in A^{\tau\surd}$.

For any $a \in A$, define \xrightarrow{a} as $(\xrightarrow{\tau})^* \xrightarrow{a} (\xrightarrow{\tau})^*$ and $\xrightarrow{\surd}$ as $(\xrightarrow{\tau})^* \xrightarrow{\surd}$; for arbitrary strings in $A^{*\surd} = A^* \cup \{x\surd : x \in A^*\}$ define $\xrightarrow{\varepsilon}$ as $(\xrightarrow{\tau})^*$ and, for $x \in A^*$ and $y \in A^{*\surd}$, define \xrightarrow{xy} as the relational composition $\xrightarrow{x} \xrightarrow{y}$; finally, define $\xrightarrow{\tau}$ as $\xrightarrow{\tau} (\xrightarrow{\tau})^*$, the transitive closure of $\xrightarrow{\tau}$.

For a transition system with labels in A , internal actions and termination, $\mathbf{S} = \langle S, \varphi \rangle$, and $s \in S$ we put $C_s(x) = \{a \in A^\surd : \exists t, s \xrightarrow{xa} t\}$ and $I(s) = C_s(\varepsilon) = \{a \in A^\surd : \exists t, s \xrightarrow{a} t\}$; and we say that s *refuses* $X \subseteq A^\surd$ (s *ref* X) if and only if either s is a stable state (one without τ or \surd transitions) and $I(s) \cap X = \emptyset$ or $s \xrightarrow{\surd}$ and $X \subseteq A$. The set of *failures* of s is

$$\begin{aligned} Fl(s) = \{ & (x, X) \in A^* \times \mathcal{P}(A^\surd) : \exists t, s \xrightarrow{x} t \text{ and } t \text{ ref } X\} \\ & \cup \{(x\surd, X) \in A^{*\surd} \times \mathcal{P}(A^\surd) : \exists t, s \xrightarrow{x\surd} t\}; \end{aligned}$$

and the set of *refusal* of s is

$$Rf(s) = \{X : (\varepsilon, X) \in Fl(s)\}.$$

As for traces and failures without termination, for failures with termination we have $I(s) = I(f(s))$ for $f : \mathbf{S}_1 \rightarrow \mathbf{S}_2$, an arbitrary weak morphism, and $s \in S_1$.

Lemma 10. *If $f : \mathbf{S}_1 \rightarrow \mathbf{S}_2$ is a weak morphism and $s \in S_1$, then $Fl(s) = Fl(f(s))$. In particular, $Rf(s) = Rf(f(s))$.*

Proof. The proof is similar to Lemma 1. Just notice that, as f is a weak morphism, for every $a \in A^{\tau\surd}$, $s \xrightarrow{a}$ iff $f(s) \xrightarrow{a}$; and

$$\begin{aligned} Fl(s) = \{ & (x, X) \in A^* \times \mathcal{P}(A^\surd) : \exists t, s \xrightarrow{x} t \not\xrightarrow{\tau, \surd} \text{ and } I(t) \cap X = \emptyset\} \\ & \cup \{(x, X) \in A^* \times \mathcal{P}(A) : \exists t, s \xrightarrow{x} t \xrightarrow{\surd}\} \\ & \cup \{(x\surd, X) \in A^{*\surd} \times \mathcal{P}(A^\surd) : \exists t, s \xrightarrow{x\surd} t\}. \end{aligned}$$

A failure set over A^\surd is any set $P \subseteq A^{*\surd} \times \mathcal{P}(A^\surd)$ such that the following conditions holds:

F1 through **F4**

F5 $(x\surd, \emptyset) \in P \wedge X \subseteq A \Rightarrow (x, X) \in P$.

F6 $(x\surd, \emptyset) \in P \wedge X \subseteq A^\surd \Rightarrow (x\surd, X) \in P$.

Let \mathcal{F} be the set of all failure sets over A^\vee . We turn \mathcal{F} into a transition system $F = \langle \mathcal{F}, \zeta_{Fl} \rangle$ by defining the transitions associated with ζ_{Fl} as follows. Let P and Q be failure-sets; we write with $a \in A^\vee$

$$\begin{aligned} P \xrightarrow{\tau} Q & \text{ iff } Q \subsetneq P; \\ P \xrightarrow{a} Q & \text{ iff } Q \subseteq \partial_a(P). \end{aligned}$$

Remark 2. If $P \xrightarrow{\vee} Q$ then by **F1** $(\varepsilon, \emptyset) \in Q$ and $(\vee, \emptyset) \in P$. By **F6** $(\vee, X) \in P$, for all $X \subseteq A^\vee$ and it follows that $\partial_\vee(P) = \{(\varepsilon, X) : X \subseteq A^\vee\}$. By **F4** there is no failure set over A^\vee such that $Q \subsetneq \partial_\vee(P)$ and then,

$$P \xrightarrow{\vee} Q \text{ iff } Q = \{(\varepsilon, X) : X \subseteq A^\vee\} \text{ and } \forall X \subseteq A^\vee, (\vee, X) \in P;$$

and

$$\{(\varepsilon, X) : X \subseteq A^\vee\} \not\rightarrow.$$

Lemma 11. *If $(P_i)_{i \in I}$ is a nonempty family of failure sets over A^\vee , $\bigcup_{i \in I} P_i$ is a failure set over A^\vee .*

Proof. Conditions **F1** through **F4** have been verified in Lemma 9 and conditions **F5** and **F6** are easy to check.

Lemma 12. *The transition system $F = \langle \mathcal{F}, \zeta_{Fl} \rangle$ is transitive.*

Proof. See Lemma 2.

Lemma 13. *If $(a, \emptyset) \in P$, then $Q = \{(x, X) : (ax, X) \in P\}$ is in \mathcal{F} and $P \xrightarrow{a} Q$. For any $R \in \mathcal{F}$ such that $P \xrightarrow{a} R$, we have $Q \xrightarrow{\varepsilon} R$.*

Proof. By Lemma 3 the only conditions remaining to prove are **F5** and **F6**, which are easy to check.

Lemma 14. *Let $P \in \mathcal{F}$ and $x \in A^*$.*

1. *For any $Q \in \mathcal{F}$, $P \xrightarrow{x} Q$ iff for every $(y, X) \in Q$, $(xy, X) \in P$.*
2. *If $(x, \emptyset) \in P$, then $Q = \{(y, X) : (xy, X) \in P\}$ is in \mathcal{F} and $P \xrightarrow{x} Q$. For any $R \in \mathcal{F}$ such that $P \xrightarrow{x} R$, we have $Q \xrightarrow{\varepsilon} R$.*

Proof. See Lemma 4.

Lemma 15. *Let P be a failure-set. In $F = \langle \mathcal{F}, \zeta_{Fl} \rangle$ the following equalities hold:*

1. $\text{Tr}(P) = \{x \in A^{*\vee} : (x, \emptyset) \in P\}$.
2. $C_P(x) = \{a \in A^\vee : (xa, \emptyset) \in P\}$.
3. $I(P) = \{a \in A^\vee : (a, \emptyset) \in P\}$.

Proof. See Lemma 5

Lemma 16. *If $P \in \mathcal{F}$ and $(\varepsilon, X) \in P$, then*

$$Q = \{(\varepsilon, Y) : (\varepsilon, X \cup Y) \in P\} \cup \{(ax, Y) \in P : a \notin X\}$$

is in \mathcal{F} , $P \xrightarrow{\varepsilon} Q$ and $I(Q) \cap X = \emptyset$. For any $R \in \mathcal{F}$ such that $P \xrightarrow{\varepsilon} R$ and $I(R) \cap X = \emptyset$, we have $Q \xrightarrow{\varepsilon} R$.

Proof. By Lemma 6 Q satisfies **F1** through **F4**. For **F5** let $(x\checkmark, \emptyset) \in Q$ and $Y \subseteq A$; if $x = \varepsilon$ then $(\checkmark, \emptyset) \in P$ and $\checkmark \notin X$; since P satisfies **F5**, $(\varepsilon, Z) \in P$ for every $Z \subseteq A$, in particular $(\varepsilon, X \cup Y) \in P$ and $(\varepsilon, Y) \in Q$. If $x = ay$ then $(x\checkmark, \emptyset) \in P$ and $a \notin X$, since P satisfies **F5**, $(x, Y) \in P$ and, by definition of Q , $(x, Y) \in Q$ as required. The verification of **F6** is similar to **F5**. For the last condition see Lemma 6.

Lemma 17. *If P is failure set over A^\checkmark ,*

$$\begin{aligned} \tilde{P} = & \{(x, X) : (x, X) \in P \text{ and } \forall y \leq x, (y\checkmark, \emptyset) \notin P\} \\ & \cup \{(x, X) : (x\checkmark, \emptyset) \in P, X \subseteq A \text{ and } \forall y < x, (y\checkmark, \emptyset) \notin P\} \\ & \cup \{(x\checkmark, X) : (x\checkmark, \emptyset) \in P, X \subseteq A^\checkmark \text{ and } \forall y < x, (y\checkmark, \emptyset) \notin P\} \end{aligned}$$

is failure set over A^\checkmark and $P \xrightarrow{\varepsilon} \tilde{P}$.⁶

Proof. Let $Q_1 = \{(x, X) : (x, X) \in P \text{ and } \forall y \leq x, (y\checkmark, \emptyset) \notin P\}$, $Q_2 = \{(x, X) : (x\checkmark, \emptyset) \in P, X \subseteq A \text{ and } \forall y < x, (y\checkmark, \emptyset) \notin P\}$ and $Q_3 = \{(x\checkmark, X) : (x\checkmark, \emptyset) \in P, X \subseteq A^\checkmark \text{ and } \forall y < x, (y\checkmark, \emptyset) \notin P\}$.

If $(\checkmark, \emptyset) \in P$ then $(\varepsilon, \emptyset) \in Q_2$ otherwise $(\varepsilon, \emptyset) \in Q_1$, so Q verifies **F1**. For **F2** let $(xy, \emptyset) \in Q$ and $y \neq \varepsilon$; if $(xy, \emptyset) \in Q_1$ then $(x, \emptyset) \in Q_1$; if $(xy, \emptyset) \in Q_2$ then, by **F2**, $(x, \emptyset) \in P$ and $\forall w \leq x, (w\checkmark, \emptyset) \notin P$, so $(x, \emptyset) \in Q_1$; if $(xy, \emptyset) \in Q_3$ either $y = \checkmark$ and $\forall w < x, (w\checkmark, \emptyset) \notin P$ or $y = w\checkmark$ with $w \neq \varepsilon$ and $\forall w \leq x, (w\checkmark, \emptyset) \notin P$; in the first case $(x, \emptyset) \in Q_2$ and in the second case, since by **F2** $(x, \emptyset) \in P$, $(x, \emptyset) \in Q_1$. The condition **F3** is easy to check. For **F4** let $(x, X) \in Q$ and $Y \neq \emptyset$ such that $\forall a \in Y, (xa, \emptyset) \notin Q$. If $(x, X) \in Q_1$, first we prove that $\forall a \in Y, (xa, \emptyset) \notin P$. Note that, by definition of Q_1 , $(x\checkmark, \emptyset) \notin P$ and for every $a \in A$, $\forall y < xa, (y\checkmark, \emptyset) \notin P$. Suppose that there is $a \in Y$ such that $(xa, \emptyset) \in P$ then, since $(x, \emptyset) \in Q_1$ and $(xa, \emptyset) \notin Q_1$, we must have $(xa\checkmark, \emptyset) \in P$ and then $(xa, \emptyset) \in Q_2 \subseteq Q$, this leads to a contradiction; applying **F4** to P , $(x, X \cup Y) \in P$ and $(x, X \cup Y) \in Q_1$. If $(x, X) \in Q_2$ then $X \subseteq A$, $(x\checkmark, \emptyset) \in P$ and $(x, W) \in Q_2$ for every $W \subseteq A$. We also have $(x\checkmark, \emptyset) \in Q_3$, then $\checkmark \notin Y \subseteq A$ and $(x, X \cup Y) \in Q_2$. If $(x, X) \in Q_3$ then $(x, W) \in Q_3$ for all $W \subseteq A^\checkmark$, in particular for $W = X \cup Y$. Conditions **F5** and **F6** are a easy to check. By construction $Q_1 \subseteq P$ and, if $(x\checkmark, \emptyset) \in P$, by **F5** and **F6**, $(x, X) \in P$ and $(x\checkmark, Y) \in P$ for every $X \subseteq A$ and $Y \subseteq A^\checkmark$, thus $Q_2, Q_3 \subseteq P$ and $\tilde{P} \subseteq P$.

Lemma 18. *If P is failure set over A^\checkmark ,*

$$Q = \{(x, X) : (x, X) \in \tilde{P} \text{ and } \forall a \in X, (xa, \emptyset) \notin \tilde{P}\}$$

is a failure set over A^\checkmark and $P \xrightarrow{\varepsilon} Q \xrightarrow{\checkmark}$.

⁶ y is a initial subsequence of x , $y \leq x$, if $x = yw$ for some w ; y is a proper initial subsequence of x , $y < x$, if $x = yw$ for some $w \neq \varepsilon$.

Proof. By Lemma 17 \tilde{P} is a failure set over A^\vee and $\tilde{P} \subseteq P$. Note that $(x, \emptyset) \in Q$ iff $(x, \emptyset) \in \tilde{P}$. Axioms **F1** through **F3** are easy to check. For **F4** let $(x, X) \in Q$ and Y such that $\forall a \in Y, (xa, \emptyset) \notin Q$. Then $(x, X) \in \tilde{P}$ and $\forall a \in Y, (xa, \emptyset) \notin \tilde{P}$; by **F4**, $(x, X \cup Y) \in \tilde{P}$. Together with $\forall a \in X \cup Y, (xa, \emptyset) \notin \tilde{P}$ this implies that $(x, X \cup Y) \in Q$. For **F5** let $(x\checkmark, \emptyset) \in Q$ then $(x\checkmark, \emptyset) \in \tilde{P}$; by definition of \tilde{P} , $(x\checkmark, X) \in \tilde{P}$ for every $X \subseteq A$ and $(xa, \emptyset) \notin \tilde{P}$ for every $a \in A$, so we conclude that $(x\checkmark, X) \in Q$ for every $X \subseteq A$. The verification of **F6** is similar to the verification of **F5**.

Lemma 19. *Let P be a failure-set. In $F = \langle \mathcal{F}, \zeta_{Fl} \rangle$ the following equalities hold:*

1. $Rf(P) = \{X \subseteq A^\vee : (\varepsilon, X) \in P\}$.
2. $Fl(P) = P$.

Proof. 1. If $X \in Rf(P)$, there is Q such that $P \xrightarrow{\varepsilon} Q$ and either $Q \not\xrightarrow{\checkmark, \tau}$ and $I(Q) \cap X = \emptyset$ or $Q \xrightarrow{\checkmark}$ and $X \subseteq A$. The first case was already seen in Lemma 8. In the second case, by Remark 2, $(\checkmark, \emptyset) \in Q \subseteq P$ and, by **F5**, $(\varepsilon, X) \in P$ for every $X \subseteq A$. Conversely, if $(\varepsilon, X) \in P$, there is Q such that $P \xrightarrow{\varepsilon} Q$ and $I(Q) \cap X = \emptyset$, by Lemma 16; by Lemma 18, there is a R such that $Q \xrightarrow{\varepsilon} R \not\xrightarrow{\checkmark}$, hence $P \xrightarrow{\varepsilon} R$ and $I(R) \cap X = \emptyset$. If $R \not\xrightarrow{\checkmark}$ by definition $X \in Rf(P)$. If $R \xrightarrow{\checkmark}$, $\checkmark \in I(R)$ and $X \subseteq A$ then $X \in Rf(P)$.

2. Let $(x, X) \in Fl(P)$ then, there is a Q such that $P \xrightarrow{x} Q$. We have three cases, either $x \in A^*$, $Q \not\xrightarrow{\checkmark, \tau}$ and $I(Q) \cap X = \emptyset$ or $x \in A^*$, $Q \xrightarrow{\checkmark}$ and $X \subseteq A$; or $x = y\checkmark$ and $X \subseteq A^\vee$. In the first two cases we conclude that $X \in Rf(Q)$, so $(\varepsilon, X) \in Q$; in the last case, by Remark 2, $(\varepsilon, X) \in Q$; in which case, by the first statement of Lemma 14, $(x, X) \in P$. Conversely, let $(x, X) \in P$; by **F3**, $(x, \emptyset) \in P$, so by the second statement of Lemma 14, there is Q such that $P \xrightarrow{x} Q$ and $(\varepsilon, X) \in Q$, so $X \in Rf(Q)$ and, there is R such that $Q \xrightarrow{\varepsilon} R \not\xrightarrow{\checkmark}$ and either $R \not\xrightarrow{\checkmark}$ and $I(R) \cap X = \emptyset$ or $R \xrightarrow{\checkmark}$ and $X \subseteq A$. Together with $P \xrightarrow{x} Q$, this implies that $(x, X) \in Fl(P)$.

From Lemma 10 and Lemma 19 we conclude that $F = \langle \mathcal{F}, \zeta_{Fl} \rangle$ is quasi-final with respect to behaviour Fl .

For an arbitrary transition system with termination $S = \langle S, \varphi \rangle$ and any $s \in S$, (6) can be generalized as follows:

$$Fl(s) = N(s) \cup N_{\checkmark}(s) \cup \bigcup_{a \in A} a \cdot \bigcup_{s \xrightarrow{a} s'} Fl(s') \quad (10)$$

where

$$N(s) = \{(\varepsilon, X) : \exists s' \forall a \in X, s \xrightarrow{\varepsilon} s' \not\xrightarrow{a}\} \cup \{(\varepsilon, X) : X \subseteq A \text{ and } s \not\xrightarrow{\checkmark}\} \quad (11)$$

$$N_{\checkmark}(s) = \{(\checkmark, X) : X \subseteq A^\vee \text{ and } s \not\xrightarrow{\checkmark}\}. \quad (12)$$

3.5 The Failure Semantics of CSP

The syntax of basic CSP processes is given by the following grammar:

Proc ::=	<i>STOP</i>	% deadlock process
	<i>SKIP</i>	% terminating process
	$a \longrightarrow \text{Proc}$	% action prefix
	$?x : X \longrightarrow \text{Proc}$	% prefix choice
	$\text{Proc} \square \text{Proc}$	% external choice
	$\text{Proc} \sqcap \text{Proc}$	% internal choice
	$\text{Proc} \parallel \text{Proc}$	% generalized parallel
	$\text{Proc} \overset{X}{\parallel} \text{Proc}$	% alphabetized parallel
	$\text{Proc} \parallel \text{Proc}$	% synchronous parallel
	$\text{Proc} \parallel \text{Proc}$	% interleaving
	$\text{Proc} ; \text{Proc}$	% sequential composition
	$\text{Proc} \setminus X$	% hiding
	$\text{Proc} [[R]]$	% relational renaming
	if φ then Proc else Proc	% boolean conditional

with A the alphabet, $X, Y \subseteq A$ and $R \subseteq A \times A$ a binary relation. The grammar is extended by $\text{Proc} ::= \text{ProcName} \mid \text{ProcName}(x)$, where x is a variable over A .

The set of inference rules for the CSP transition system is given below. In this rules we consider $a, b \in A$, $x \in A^\tau = A \cup \{\tau\}$, $y \in A^\surd = A \cup \{\surd\}$ and $z \in A^{\tau\surd} = A \cup \{\tau, \surd\}$; Ω denotes any terminated process.

Deadlock process

“no rules for STOP”

Terminating process

$$\overline{SKIP \xrightarrow{\surd} \Omega}$$

Action prefix

$$\frac{}{(a \longrightarrow P) \xrightarrow{a} P} \quad \frac{P \xrightarrow{\tau} P'}{(a \longrightarrow P) \xrightarrow{\tau} (a \longrightarrow P')}$$

Prefix choice

$$\frac{}{(?x : X \longrightarrow P) \xrightarrow{a} P[a/x]} \quad (a \in X)$$

External choice

$$\frac{P \xrightarrow{\tau} P'}{P \square Q \xrightarrow{\tau} P' \square Q} \quad \frac{Q \xrightarrow{\tau} Q'}{P \square Q \xrightarrow{\tau} P \square Q'}$$

$$\frac{P \xrightarrow{y} P'}{P \sqcap Q \xrightarrow{y} P'} \quad \frac{Q \xrightarrow{y} Q'}{P \sqcap Q \xrightarrow{y} Q'}$$

Internal choice

$$\overline{P \sqcap Q \xrightarrow{\tau} P} \quad \overline{P \sqcap Q \xrightarrow{\tau} Q}$$

Generalized parallel

$$\frac{P \xrightarrow{\tau} P'}{P \parallel_X Q \xrightarrow{\tau} P' \parallel_X Q} \quad \frac{Q \xrightarrow{\tau} Q'}{P \parallel_X Q \xrightarrow{\tau} P \parallel_X Q'}$$

$$\frac{P \xrightarrow{a} P'}{P \parallel_X Q \xrightarrow{a} P' \parallel_X Q} \quad (a \notin X) \quad \frac{Q \xrightarrow{a} Q'}{P \parallel_X Q \xrightarrow{a} P \parallel_X Q'} \quad (a \notin X)$$

$$\frac{P \xrightarrow{a} P' \quad Q \xrightarrow{a} Q'}{P \parallel_X Q \xrightarrow{a} P' \parallel_X Q'} \quad (a \in X)$$

$$\frac{P \xrightarrow{\checkmark} P' \quad Q \xrightarrow{\checkmark} Q'}{P \parallel_X Q \xrightarrow{\checkmark} \Omega}$$

Alphabetized parallel

$$\frac{P \xrightarrow{\tau} P'}{P_{X \parallel Y} Q \xrightarrow{\tau} P'_{X \parallel Y} Q} \quad \frac{Q \xrightarrow{\tau} Q'}{P_{X \parallel Y} Q \xrightarrow{\tau} P_{X \parallel Y} Q'}$$

$$\frac{P \xrightarrow{a} P'}{P_{X \parallel Y} Q \xrightarrow{a} P'_{X \parallel Y} Q} \quad (a \in X \setminus Y)$$

$$\frac{Q \xrightarrow{a} Q'}{P_{X \parallel Y} Q \xrightarrow{a} P_{X \parallel Y} Q'} \quad (a \in Y \setminus X)$$

$$\frac{P \xrightarrow{a} P' \quad Q \xrightarrow{a} Q'}{P_{X \parallel Y} Q \xrightarrow{a} P'_{X \parallel Y} Q'} \quad (a \in X \cap Y)$$

$$\frac{P \xrightarrow{\checkmark} P' \quad Q \xrightarrow{\checkmark} Q'}{P_{X \parallel Y} Q \xrightarrow{\checkmark} \Omega}$$

Synchronous parallel

$$\frac{P \xrightarrow{\tau} P'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q} \quad \frac{Q \xrightarrow{\tau} Q'}{P \parallel Q \xrightarrow{\tau} P \parallel Q'}$$

$$\frac{P \xrightarrow{a} P' \quad Q \xrightarrow{a} Q'}{P \parallel Q \xrightarrow{a} P' \parallel Q'}$$

$$\frac{Q \xrightarrow{\surd} Q' \quad P \xrightarrow{\surd} P'}{P \parallel Q \xrightarrow{\surd} \Omega}$$

Interleaving

$$\frac{P \xrightarrow{x} P' \quad Q \xrightarrow{x} Q'}{P \parallel Q \xrightarrow{x} P' \parallel Q'}$$

$$\frac{P \xrightarrow{\surd} P' \quad Q \xrightarrow{\surd} Q'}{P \parallel Q \xrightarrow{\surd} \Omega}$$

Sequential composition

$$\frac{P \xrightarrow{x} P'}{P; Q \xrightarrow{x} P'; Q} \quad \frac{P \xrightarrow{\surd} P'}{P; Q \xrightarrow{\tau} Q}$$

Hiding

$$\frac{P \xrightarrow{x} P'}{P \setminus X \xrightarrow{x} P' \setminus X} \quad (x \notin X) \quad \frac{P \xrightarrow{a} P'}{P \setminus X \xrightarrow{\tau} P' \setminus X} \quad (a \in X)$$

$$\frac{P \xrightarrow{\surd} P'}{P \setminus X \xrightarrow{\surd} \Omega}$$

Renaming

$$\frac{P \xrightarrow{\tau} P'}{P[[R]] \xrightarrow{\tau} P'[[R]]} \quad \frac{P \xrightarrow{a} P'}{P[[R]] \xrightarrow{b} P'[[R]]} \quad (aRb)$$

$$\frac{P \xrightarrow{\surd} P'}{P[[R]] \xrightarrow{\surd} \Omega}$$

Boolean conditional

$$\frac{P \xrightarrow{z} P'}{\text{if } \varphi \text{ then } P \text{ else } Q \xrightarrow{z} P'} \quad (\varphi \text{ evaluates to true})$$

$$\frac{Q \xrightarrow{z} Q'}{\text{if } \varphi \text{ then } P \text{ else } Q \xrightarrow{z} Q'} \quad (\varphi \text{ evaluates to false})$$

The transition rules allow to define an operational and a denotational semantics assigning to each process term a behaviour which in the case we have been considering is a failure-set. To prove the two semantics coincide, we have to show that every operator (binary or otherwise) satisfies the appropriate version of (4). This is the contents of our next result.

Proposition 2. For all $t, u \in TZ$,

1. $Fl(a \longrightarrow t) = Fl(a \longrightarrow Fl(t))$ % action prefix
2. $Fl(?x : K \longrightarrow t) = Fl(?x : K \longrightarrow Fl(t))$ % prefix choice
3. $Fl(t \sqcap u) = Fl(Fl(t) \sqcap Fl(u))$ % external choice
4. $Fl(t \sqcap u) = Fl(Fl(t) \sqcap Fl(u))$ % internal choice
5. $Fl(t \parallel u) = Fl(Fl(t) \parallel Fl(u))$ % generalized parallel
6. $Fl(t \overset{K}{\parallel}_{K_1} \parallel_{K_2} u) = Fl(\overset{K}{Fl(t)} \parallel_{K_1} \parallel_{K_2} Fl(u))$ % alphbetized parallel
7. $Fl(t \parallel u) = Fl(Fl(t) \parallel Fl(u))$ % synchronous parallel
8. $Fl(t \parallel\parallel u) = Fl(Fl(t) \parallel\parallel Fl(u))$ % interleaving
9. $Fl(t ; u) = Fl(Fl(t) ; Fl(u))$ % sequential compositon
10. $Fl(t \setminus K) = Fl(Fl(t) \setminus K)$ % hiding
11. $Fl(t \llbracket R \rrbracket) = Fl(Fl(t) \llbracket R \rrbracket)$ % renaming
12. $Fl(\text{if } \varphi \text{ then } t \text{ else } u) = Fl(\text{if } \varphi \text{ then } Fl(t) \text{ else } Fl(u))$ % boolean conditional

Proof.

1. Action prefix

$$\begin{aligned} Fl(a \longrightarrow t) &= \{(\varepsilon, X) : a \notin X\} \cup a \cdot Fl(t) \\ &= \{(\varepsilon, X) : a \notin X\} \cup a \cdot Fl(Fl(t)) \\ &= Fl(a \longrightarrow Fl(t)) \end{aligned}$$

2. Prefix choice

$$\begin{aligned} Fl(?k : K \longrightarrow t) &= \{(\varepsilon, X) : X \cap K = \emptyset\} \cup \bigcup_{a \in K} a \cdot Fl(t[a/k]) \\ &= \{(\varepsilon, X) : X \cap K = \emptyset\} \cup \bigcup_{a \in K} a \cdot Fl(Fl(t)[a/k]) \\ &= Fl(?k : K \longrightarrow Fl(t)) \end{aligned}$$

Note that $Fl(t) = \lambda a. Fl(t[a/k])$

3. External choice

$$\begin{aligned} Fl(t \sqcap u) &= \{(\varepsilon, X) : (\varepsilon, X) \in Fl(t) \cap Fl(u)\} \cup \{(\varepsilon, X) : X \subseteq A \wedge (t \overset{\checkmark}{\Rightarrow} \vee u \overset{\checkmark}{\Rightarrow})\} \\ &\quad \cup \{(\checkmark, X) : X \subseteq A^\checkmark \wedge (t \overset{\checkmark}{\Rightarrow} \vee u \overset{\checkmark}{\Rightarrow})\} \cup \bigcup_{a \in A} a \cdot \partial_a(Fl(t) \cup Fl(u)) \\ &= \{(\varepsilon, K) : (\varepsilon, K) \in Fl(Fl(t)) \cap Fl(Fl(u))\} \\ &\quad \cup \{(\varepsilon, X) : X \subseteq A \wedge (Fl(t) \overset{\checkmark}{\Rightarrow} \vee Fl(u) \overset{\checkmark}{\Rightarrow})\} \\ &\quad \cup \{(\checkmark, X) : X \subseteq A^\checkmark \wedge (Fl(t) \overset{\checkmark}{\Rightarrow} \vee Fl(u) \overset{\checkmark}{\Rightarrow})\} \\ &\quad \cup \bigcup_{a \in A} a \cdot \partial_a(Fl(Fl(t)) \cup Fl(Fl(u))) \\ &= Fl(Fl(t) \sqcap Fl(u)) \end{aligned}$$

4. Internal choice

$$\begin{aligned} Fl(t \sqcap u) &= Fl(t) \cup Fl(u) \\ &= Fl(Fl(t)) \cup Fl(Fl(u)) \\ &= Fl(Fl(t) \sqcap Fl(u)) \end{aligned}$$

5. Generalized parallel

We prove by induction on the length of failures⁷ that both sides of the equality have the same failures of any given length. First note that, with $a \in A^\vee$, $t \parallel_K u \xrightarrow{a} t' \parallel_K u'$ iff $a \in K \cup \{\checkmark\}$ and $t \xrightarrow{a} t' \wedge u \xrightarrow{a} u'$, or $a \notin K \cup \{\checkmark\}$ and either $t \xrightarrow{a} t' \wedge u \xrightarrow{\checkmark} u'$ or $t \xrightarrow{\checkmark} t' \wedge u \xrightarrow{a} u'$, and that $t \parallel_K u \not\xrightarrow{a}$ iff $a \in K \cup \{\checkmark\}$ and $t \not\xrightarrow{a} t' \vee u \not\xrightarrow{a} u'$, or $a \notin K \cup \{\checkmark\}$ and $t \not\xrightarrow{a} \wedge u \not\xrightarrow{a}$. By (10),

$$\begin{aligned} Fl(t \parallel_K u) &= N(t \parallel_K u) \cup N_{\checkmark}(t \parallel_K u) \cup \bigcup_{a \in K} a \cdot \left(\bigcup_{\substack{t \xrightarrow{a} t' \\ u \xrightarrow{a} u'}} Fl(t' \parallel_K u') \right) \\ &\cup \bigcup_{a \in A \setminus K} a \cdot \left(\bigcup_{\substack{t \xrightarrow{a} t' \\ u \xrightarrow{\checkmark} u'}} Fl(t' \parallel_K u') \cup \bigcup_{\substack{t \xrightarrow{\checkmark} t' \\ u \xrightarrow{a} u'}} Fl(t' \parallel_K u') \right), \end{aligned} \quad (13)$$

where by (11) and (12),

$$\begin{aligned} N(t \parallel_K u) &= \{(\varepsilon, X) : \text{exists } t', u' \text{ such that } t \xrightarrow{\checkmark} t', u \xrightarrow{\checkmark} u', \\ &\quad \forall a \in X \cap (K \cup \{\checkmark\}), t' \not\xrightarrow{a} \vee u' \not\xrightarrow{a} \\ &\quad \text{and } \forall a \in X \setminus (K \cup \{\checkmark\}), t' \not\xrightarrow{a} \wedge u' \not\xrightarrow{a}\} \\ &\cup \{(\varepsilon, X) : X \subseteq A \wedge t \not\xrightarrow{\checkmark} \wedge u \not\xrightarrow{\checkmark}\} \end{aligned}$$

and

$$N_{\checkmark}(t \parallel_K u) = \{(\checkmark, X) : X \subseteq A^\vee \wedge t \not\xrightarrow{\checkmark} \wedge u \not\xrightarrow{\checkmark}\}$$

On the other hand, since $Fl(t) \xrightarrow{a} P$ iff $P \subseteq \partial_a(Fl(t))$ and $Fl(u) \xrightarrow{\checkmark} P$ iff $P \subseteq Fl(t)$.

$$\begin{aligned} Fl(Fl(t) \parallel_K Fl(u)) &= N(Fl(t) \parallel_K Fl(u)) \cup N_{\checkmark}(Fl(t) \parallel_K Fl(u)) \\ &\cup \bigcup_{a \in K} a \cdot \left(\bigcup_{\substack{P \subseteq \partial_a(Fl(t)) \\ Q \subseteq \partial_a(Fl(u))}} Fl(P \parallel_K Q) \right) \\ &\cup \bigcup_{a \in A \setminus K} a \cdot \left(\bigcup_{\substack{P \subseteq \partial_a(Fl(t)) \\ Q \subseteq Fl(u)}} Fl(P \parallel_K Q) \right) \\ &\cup \bigcup_{a \in A \setminus K} a \cdot \left(\bigcup_{\substack{P \subseteq Fl(t) \\ Q \subseteq \partial_a(Fl(u))}} Fl(P \parallel_K Q) \right). \end{aligned}$$

⁷ The length of (x, X) is the length of x .

where

$$\begin{aligned}
N(Fl(t) \parallel_K Fl(u)) &= \{(\varepsilon, X) : \text{exists } P \subseteq Fl(t) \text{ and } Q \subseteq Fl(u) \text{ such that} \\
&\quad \forall a \in X \cap (K \cup \{\checkmark\}), P \not\stackrel{a}{\subseteq} \vee Q \not\stackrel{a}{\subseteq} \\
&\quad \text{and } \forall a \in X \setminus (K \cup \{\checkmark\}), P \not\stackrel{a}{\subseteq} \wedge Q \not\stackrel{a}{\subseteq}\} \\
&\cup \{(\varepsilon, X) : X \subseteq A \wedge Fl(t) \stackrel{\checkmark}{\subseteq} \wedge Fl(u) \stackrel{\checkmark}{\subseteq}\}
\end{aligned}$$

and

$$N_{\checkmark}(Fl(t) \parallel_K Fl(u)) = \{(\checkmark, X) : X \subseteq A^{\checkmark} \wedge Fl(t) \stackrel{\checkmark}{\subseteq} \wedge Fl(u) \stackrel{\checkmark}{\subseteq}\}$$

Note that N_{\checkmark} is the same in both cases because $Fl(t) \stackrel{a}{\subseteq}$ iff $(a, \emptyset) \in Fl(t)$, iff $t \stackrel{a}{\subseteq}$ for all $a \in A^{\checkmark}$. We first prove that $Fl(t \parallel_K u)$ is contained in $Fl(Fl(t) \parallel_K Fl(u))$.

The base of the induction holds because if $t \stackrel{\varepsilon}{\subseteq} t'$ then $Fl(t') \subseteq Fl(t)$. Assume the result for all failures of length n and take a failure $(ax, X) \in Fl(t \parallel_K u)$ of length $n+1$, that is, $a \in A^{\checkmark}$ and $x \in A^{*\checkmark}$ has length n . If $a \neq \checkmark$, by (10), there exist t', u' such that $t \parallel_K u \stackrel{a}{\subseteq} t' \parallel_K u'$ and $(x, X) \in Fl(t' \parallel_K u')$, and by induction hypothesis, (x, X) is in $Fl(Fl(t') \parallel_K Fl(u'))$. There are three possibilities, if $a \in A \setminus K$, $t \stackrel{a}{\subseteq} t'$ and $u \stackrel{\varepsilon}{\subseteq} u'$ imply $Fl(t') \subseteq \partial_a(Fl(t))$ and $Fl(u') \subseteq Fl(u)$, respectively, so $Fl(Fl(t') \parallel_K Fl(u'))$ is one of the $Fl(P \parallel_K Q)$ with $P \subseteq \partial_a(Fl(t))$ and $Q \subseteq Fl(u)$. It follows that (ax, X) is in $Fl(Fl(t) \parallel_K Fl(u))$. The other cases are similar. If $a = \checkmark$ ($ax = \checkmark$) the result comes out because N_{\checkmark} is the same in both cases. The proof of the converse will be based on the following result:

$$P \subseteq \partial_x(Fl(t)), \quad Q \subseteq \partial_y(Fl(u)) \quad \text{imply} \quad Fl(P \parallel_K Q) \subseteq \bigcup_{\substack{t \stackrel{x}{\subseteq} t' \\ u \stackrel{y}{\subseteq} u'}} Fl(t' \parallel_K u'). \quad (14)$$

Assuming (14), a simple case analysis shows that $Fl(Fl(t) \parallel_K Fl(u))$ is contained in $Fl(t \parallel_K u)$. Indeed, both sets have the same N_{\checkmark} and the same failures of length zero, this can be seen putting $x = y = \varepsilon$ in (14). For any $Fl(P \parallel_K Q)$ such that for $a \in A \setminus K$, $P \subseteq \partial_a(Fl(t))$ and $Q \subseteq Fl(u) = \partial_{\varepsilon}(Fl(u))$ is contained in $\bigcup_{\substack{t \stackrel{a}{\subseteq} t' \\ u \stackrel{\varepsilon}{\subseteq} u'}} Fl(t' \parallel_K u')$, by (14), and a similar situation occurs if $P \subseteq Fl(t) = \partial_{\varepsilon}(Fl(t))$ and $Q \subseteq \partial_a(Fl(u))$ or if $a \in K$, $P \subseteq \partial_a(Fl(t))$ and $Q \subseteq \partial_a(Fl(u))$.

We prove (14) again by induction on the length of failures; specifically, for all n and all t, u, x, y, P and Q satisfying the premisses, the inclusion in the

conclusion holds for all failures of length n . The reasoning will be based on the following instance of (13):

$$\begin{aligned} Fl(P \parallel_K Q) &= N(P \parallel_K Q) \cup N_{\checkmark}(P \parallel_K Q) \cup \bigcup_{a \in K} a \cdot \left(\bigcup_{\substack{P \xrightarrow{a} P' \\ Q \xrightarrow{a} Q'}} Fl(P' \parallel_K Q') \right) \\ &\cup \bigcup_{a \in A \setminus K} a \cdot \left(\bigcup_{\substack{P \xrightarrow{a} P' \\ Q \xrightarrow{a} Q'}} Fl(P' \parallel_K Q') \cup \bigcup_{\substack{P \xrightarrow{a} P' \\ Q \xrightarrow{a} Q'}} Fl(P' \parallel_K Q') \right). \end{aligned}$$

where

$$\begin{aligned} N(P \parallel_K Q) &= \{(\varepsilon, X) : \text{exists } P' \subseteq P \text{ and } Q' \subseteq Q \text{ such that} \\ &\quad \forall a \in X \cap (K \cup \{\checkmark\}), P' \not\xrightarrow{a} \vee Q' \not\xrightarrow{a} \\ &\quad \text{and } \forall a \in X \setminus (K \cup \{\checkmark\}), P' \not\xrightarrow{a} \wedge Q' \not\xrightarrow{a}\} \\ &\cup \{(\varepsilon, X) : X \subseteq A \wedge P \xrightarrow{\checkmark} \wedge Q \xrightarrow{\checkmark}\} \end{aligned}$$

and

$$N_{\checkmark}(P \parallel_K Q) = \{(\checkmark, X) : X \subseteq A^{\checkmark} \wedge P \xrightarrow{\checkmark} \wedge Q \xrightarrow{\checkmark}\}$$

So let us start with a failure (ε, X) of length zero in $Fl(P \parallel_K Q)$. If $X \subseteq A$,

$P \xrightarrow{\checkmark}$ and $Q \xrightarrow{\checkmark}$ then $(\checkmark, \emptyset) \in P \subseteq \partial_x(Fl(t))$ and by (9) there is t' such that $t \xrightarrow{x} t'$ and $(\checkmark, \emptyset) \in Fl(t')$, in the same way we have $(\checkmark, \emptyset) \in Fl(u')$ for some u' such that $u \xrightarrow{y} u'$ and it follows that $(\varepsilon, X) \in Fl(t' \parallel_K u') \subseteq \bigcup_{\substack{t \xrightarrow{x} t' \\ u \xrightarrow{y} u'}} Fl(t' \parallel_K u')$. Otherwise we have $X = X_1 \cup X_2 \cup X_3$ with $X_1, X_2 \subseteq K \cup \{\checkmark\}$, $X_3 \subseteq A \setminus K$, $(\varepsilon, X_1) \in N(P)$, $(\varepsilon, X_2) \in N(Q)$ and $(\varepsilon, X_3) \in N(P) \cap N(Q)$. By hypothesis $N(P) \subseteq P \subseteq \partial_x(Fl(t))$, so by (9) there is t' such that $t \xrightarrow{x} t'$ and $(\varepsilon, X_1), (\varepsilon, X_3) \in Fl(t')$; more specifically, $(\varepsilon, X_1), (\varepsilon, X_3) \in N(t')$, i.e., $\forall a \in X_1, t' \not\xrightarrow{a}$ and $\forall a \in X_3, t' \not\xrightarrow{a}$. Similarly, there is u' such that $u \xrightarrow{y} u'$ and $\forall a \in X_2, u' \not\xrightarrow{a}$ and $\forall a \in X_3, u' \not\xrightarrow{a}$. It follows that $(\varepsilon, X) \in N(t' \parallel_K u') \subseteq Fl(t' \parallel_K u')$; this shows (ε, X) is contained in the right side of the inclusion in (14). Now suppose (aw, X) has length $n+1$, with $a \in A^{\checkmark}$ and $w \in A^{*\checkmark}$, and is in $Fl(P \parallel_K Q)$. If $a \notin K \cup \{\checkmark\}$ and $(w, X) \in Fl(P' \parallel_K Q')$ for some $P' \subseteq \partial_a(P)$ and $Q' \subseteq Q$. We have

$$\begin{aligned} P' &\subseteq \partial_a(P) \subseteq \partial_a(\partial_x(Fl(t))) = \partial_{xa}(Fl(t)), \\ Q' &\subseteq Q \subseteq \partial_y(Fl(u)). \end{aligned}$$

By induction hypothesis, $(w, X) \in Fl(t'' \parallel_K u'')$ for some t'', u'' such that $t \xrightarrow{xa} t''$ and $u \xrightarrow{y} u''$. If we let t' be such that $t \xrightarrow{x} t' \xrightarrow{a} t''$ and put $u' = u''$, then

$t' \parallel_K u' \stackrel{a}{\Rightarrow} t'' \parallel_K u''$, hence $(aw, X) \in Fl(t' \parallel_K u')$, as required. For the case $a = \checkmark$ ($aw = \checkmark$), first note that $(\checkmark, X) \in Fl(t \parallel_K u) \iff (\checkmark, X) \in Fl(t) \cap Fl(u)$. If $(\checkmark, X) \in Fl(P \parallel_K Q)$ then $(\checkmark, X) \in P \cap Q \subseteq \partial_x(Fl(t)) \cap \partial_y(Fl(u))$ and by (8) $(\checkmark, X) \in Fl(t') \cap Fl(u')$ for some t', u' such that $t \stackrel{x}{\Rightarrow} t'$ and $u \stackrel{y}{\Rightarrow} u'$, then $(\checkmark, X) \in Fl(t' \parallel_K Fl(u'))$. The other cases are similar.

6. Alphabetized parallel

$$\begin{aligned}
Fl(t \parallel_{K_1} \parallel_{K_2} u) &= N(t \parallel_{K_1} \parallel_{K_2} u) \cup N_{\checkmark}(t \parallel_{K_1} \parallel_{K_2} u) \\
&\cup \bigcup_{a \in K_1 \cap K_2} a \cdot \left(\bigcup_{\substack{t \stackrel{a}{\Rightarrow} t' \\ u \stackrel{a}{\Rightarrow} u'}} Fl(t' \parallel_{K_1} \parallel_{K_2} u') \right) \\
&\cup \bigcup_{a \in K_1 \setminus K_2} a \cdot \left(\bigcup_{\substack{t \stackrel{a}{\Rightarrow} t' \\ u \stackrel{\varepsilon}{\Rightarrow} u'}} Fl(t' \parallel_{K_1} \parallel_{K_2} u') \right) \\
&\cup \bigcup_{a \in K_2 \setminus K_1} a \cdot \left(\bigcup_{\substack{t \stackrel{\varepsilon}{\Rightarrow} t' \\ u \stackrel{a}{\Rightarrow} u'}} Fl(t' \parallel_{K_1} \parallel_{K_2} u') \right),
\end{aligned}$$

where

$$\begin{aligned}
N(t \parallel_{K_1} \parallel_{K_2} u) &= \{(\varepsilon, X) : \text{exists } t', u' \text{ such that } t \stackrel{\varepsilon}{\Rightarrow} t', u \stackrel{\varepsilon}{\Rightarrow} u', \\
&\quad \forall a \in X \cap (K_1 \cap K_2 \cup \{\checkmark\}), t' \not\stackrel{a}{\Rightarrow} u' \text{ and} \\
&\quad \forall a \in (X \cap K_1) \setminus K_2, t' \not\stackrel{a}{\Rightarrow} u' \text{ and } \forall a \in (X \cap K_2) \setminus K_1, u' \not\stackrel{a}{\Rightarrow} t'\} \\
&\cup \{(\varepsilon, X) : X \subseteq A \wedge t \stackrel{\varepsilon}{\Rightarrow} u\}
\end{aligned}$$

and

$$N_{\checkmark}(t \parallel_{K_1} \parallel_{K_2} u) = \{(\checkmark, X) : X \subseteq A^{\checkmark} \wedge t \stackrel{\checkmark}{\Rightarrow} u\}$$

Similar to generalized parallel.

7. Synchronous parallel

Generalized parallel with $K = A$.

8. Interleaving

Generalized parallel with $K = \emptyset$.

9. Sequential composition

$$\begin{aligned}
Fl(t ; u) &= \{(\varepsilon, X) : \text{exists } t', u' \text{ such that } t \stackrel{\varepsilon}{\Rightarrow} t', u \stackrel{\varepsilon}{\Rightarrow} u' \\
&\quad \text{and } \forall a \in X, (a \neq \checkmark \wedge t' \not\stackrel{a}{\Rightarrow} u') \vee (t' \stackrel{\checkmark}{\Rightarrow} u')\} \\
&\cup \bigcup_{a \in A} a \cdot \left(\bigcup_{t \stackrel{a}{\Rightarrow} t'} Fl(t' ; u) \cup \bigcup_{\substack{t \stackrel{\varepsilon}{\Rightarrow} t' \\ u \stackrel{a}{\Rightarrow} u'}} Fl(u') \right)
\end{aligned}$$

Similar to generalized parallel.

10. Hiding

$$\begin{aligned} Fl(t \setminus K) = & \{(\varepsilon, X) : \text{exists } t' \text{ such that } t \xrightarrow{\varepsilon} t' \text{ and } \forall a \in X \setminus K, t' \not\xrightarrow{a}\} \\ & \cup \{(\varepsilon, X) : X \subseteq A \wedge t \xrightarrow{\varepsilon}\} \cup \{(\checkmark, X) : X \subseteq A' \wedge t \xrightarrow{\checkmark}\} \\ & \cup \bigcup_{a \in A \setminus K} a \cdot \left(\bigcup_{t \xrightarrow{a} t'} Fl(t' \setminus K) \right) \cup \bigcup_{a \in K} \bigcup_{t \xrightarrow{a} t'} Fl(t' \setminus K) \end{aligned}$$

Similar to generalized parallel.

11. Renaming

$$\begin{aligned} Fl(t[[R]]) = & \{(\varepsilon, X) : \text{exists } t' \text{ such that } t \xrightarrow{\varepsilon} t' \text{ and } \forall b \in X, \forall aRb, t' \not\xrightarrow{a}\} \\ & \cup \{(\varepsilon, X) : X \subseteq A \wedge t \xrightarrow{\varepsilon}\} \cup \{(\checkmark, X) : X \subseteq A' \wedge t \xrightarrow{\checkmark}\} \\ & \cup \bigcup_{a \in A} \bigcup_{aRb} b \cdot \left(\bigcup_{t \xrightarrow{a} t'} Fl(t'[[R]]) \right) \end{aligned}$$

$$\begin{aligned} Fl(Fl(t)[[R]]) = & \{(\varepsilon, X) : \text{exists } P \text{ such that } P \subseteq Fl(t) \text{ and } \forall b \in X, \forall aRb, P \not\xrightarrow{a}\} \\ & \cup \{(\varepsilon, X) : X \subseteq A \wedge Fl(t) \xrightarrow{\varepsilon}\} \cup \{(\checkmark, X) : X \subseteq A' \wedge Fl(t) \xrightarrow{\checkmark}\} \\ & \cup \bigcup_{a \in A} \bigcup_{aRb} b \cdot \left(\bigcup_{P \subseteq \partial_a(Fl(t))} Fl(P[[R]]) \right) \end{aligned}$$

First prove that $Fl(t[[R]])$ is contained in $Fl(Fl(t)[[R]])$ by induction on the length of failures. The base of induction holds because $t \not\xrightarrow{a}$ iff $Fl(t) \not\xrightarrow{a}$ and if $t \xrightarrow{\varepsilon} t' \not\xrightarrow{a}$ then $Fl(t') \subseteq Fl(t)$ and $Fl(t') \not\xrightarrow{a}$. Assume that the result holds for all failures of length n and take $(bx, X) \in Fl(t[[R]])$ of length $n + 1$. Then, if $bx \neq \checkmark$ ($b \in A$), there exist $a \in A$ and t' such that $aRb, t \xrightarrow{a} t'$ and $(x, X) \in Fl(t'[[R]])$ then $Fl(t) \xrightarrow{a} Fl(t')$ and by induction hypothesis $(x, X) \in Fl(Fl(t')[[R]])$. It follows that $(bx, X) \in Fl(Fl(t)[[R]])$. For the converse we only have to prove that

$$P \subseteq \partial_x(Fl(t)) \text{ imply } Fl(P[[R]]) \subseteq \bigcup_{t \xrightarrow{x} t'} Fl(t'[[R]]).$$

The prove is done by induction on the length of failures. So let us start with failures (ε, X) of length zero in $Fl(P[[R]])$. If $X \subseteq A$ and $P \xrightarrow{\varepsilon}$ then $(\checkmark, \emptyset) \in P \subseteq \partial_x(Fl(t)) = \bigcup_{t \xrightarrow{x} t'} Fl(t')$ and $(\checkmark, \emptyset) \in Fl(t')$ for some t' such that $t \xrightarrow{x} t' \xrightarrow{\varepsilon}$ and, it follows that $(\varepsilon, X) \in Fl(t')$. If there exists a $P \subseteq Fl(t)$ such that

$$\forall b \in X \forall aRb, P \not\xrightarrow{a} \iff \forall a \in X_R, P \not\xrightarrow{a} \iff (\varepsilon, X_R) \in N(P)$$

with $X_R = \{a \in A : aRb \text{ for some } b \in X\}$. By hypothesis $N(P) \subseteq P \subseteq \partial_x(Fl(t))$, so by (9) there is t' such that $t \xrightarrow{x} t'$ and $(\varepsilon, X_R) \in Fl(t') \iff$

$(\varepsilon, X) \in Fl(t'[[R]]) \subseteq \bigcup_{t \xrightarrow{x} t'} Fl(t'[[R]])$. Suppose that $(bw, X) \in Fl(P[[R]])$ has length $n + 1$ then, if $bw \neq \checkmark$, $(w, X) \in Fl(P'[[R]])$ for some $P' \subseteq \partial_a(P)$ such that aRb . By hypothesis we have $P' \subseteq \partial_a(P) \subseteq \partial_a(\partial_x Fl(t)) \subseteq \partial_{xa} Fl(t)$ and by induction hypothesis $(w, X) \in Fl(t''[[R]])$ for some t'' such that $t \xrightarrow{xa} t''$. Let t' be such that $t \xrightarrow{x} t' \xrightarrow{a} t''$ then $(bw, X) \in Fl(t'[[R]])$. For the case $b = \checkmark$ ($bw = \checkmark$), first note that $(\checkmark, X) \in Fl(t[[R]]) \iff (\checkmark, X) \in Fl(t)$. If $(\checkmark, X) \in Fl(P[[R]])$ then $(\checkmark, X) \in P \subseteq \partial_x(Fl(t))$ and by (9) there is t' such that $t \xrightarrow{x} t'$ and $(\checkmark, X) \in Fl(t')$ then $(\checkmark, X) \in \bigcup_{t \xrightarrow{x} t'} Fl(t'[[R]])$.

12. Boolean conditional

$$\begin{aligned} Fl(\text{if } \varphi \text{ then } t \text{ else } u) &= \begin{cases} Fl(t) & , \text{ if } \varphi \text{ evaluates to true} \\ Fl(u) & , \text{ if } \varphi \text{ evaluates to false} \end{cases} \\ &= \begin{cases} Fl(Fl(t)) & , \text{ if } \varphi \text{ evaluates to true} \\ Fl(Fl(u)) & , \text{ if } \varphi \text{ evaluates to false} \end{cases} \\ &= Fl(\text{if } \varphi \text{ then } Fl(t) \text{ else } Fl(u)) \end{aligned}$$

4 Further Work

The more immediate work is to extend the failure semantics of CSP to include other semantics like infinite traces and divergences. Later we wish to consider a version of CSP with data handling capabilities, with a view to an application to the semantics of CSP-CASL [18]. Another direction is to continue to explore the expressive power of quasi-finality, and in particular to characterise all the behaviours in van Glabbeek's spectrum [6] by quasi-final objects. We also would like to find sufficient conditions that entail the equivalence of the operational and the denotational semantics, or just simplify the verification process. Finally, we would like to compare the approach based on quasi-finality with the related works mentioned in the introduction [10, 11, 12, 13, 14, 15].

References

- [1] Rutten, J., Turi, D.: Initial algebra and final coalgebra semantics for concurrency. In J.W. de Bakker, W.d.R., Rozenberg, G., eds.: A Decade of Concurrency, Reflections and Perspectives, REX School/Symposium. Number 803 in Lecture Notes in Computer Science. Springer (1994) 530–582
- [2] Turi, D., Plotkin, G.: Towards a mathematical operational semantics. In: Proc. 12th LICS Conference, IEEE, Computer Society Press (1997) 280–291
- [3] Plotkin, G.D.: A structural approach to operational semantics. Technical Report DAIMI FN-19, University of Aarhus (1981)
- [4] Hoare, C.A.R.: Communicating Sequential Processes. Series in Computer Science. Prentice-Hall International (1985)
- [5] Roscoe, A.: The Theory and Practice of Concurrency. Prentice-Hall, Englewood Cliffs, NJ (1998)

- [6] van Glabbeek, R.: The linear time–branching time spectrum I: the semantics of concrete, sequential processes. In Bergstra, J., Ponse, A., Smolka, S., eds.: *Handbook of process algebra*, Elsevier (2001) 3–99
- [7] Monteiro, L.: A coalgebraic characterization of behaviours in the linear time - branching time spectrum. In Corradini, A., Montanari, U., eds.: *Recent Trends in Algebraic Development Techniques (WADT 2008)*. Volume 5486 of *Lecture Notes in Computer Science*, Springer (2009) 250–264
- [8] Freire, E., Monteiro, L.: Defining behaviours by quasi-finality. In Oliveira, M., Woodcock, J., eds.: *Proc. SBMF'09: Brazilian Symposium on Formal Methods*. Volume 5902 of *Lecture Notes in Computer Science*, Springer (2009) 290–305
- [9] Bloom, B., Istrail, S., Meyer, A.R.: Bisimulation can't be traced. *J. ACM* **42**(1) (1995) 232–268
- [10] Power, J., Turi, D.: A coalgebraic foundation for linear time semantics. In Hofmann, M., Rosolini, G., Pavlovic, D., eds.: *CTCS '99, Conference on Category Theory and Computer Science*. Volume 29 of *Electronic Notes in Theoretical Computer Science*, Elsevier (1999) 259–274
- [11] Jacobs, B.: Trace semantics for coalgebras. In Adamek, J., Milius, S., eds.: *Coalgebraic Methods in Computer Science*. Volume 106 of *Electronic Notes in Theoretical Computer Science*, Elsevier (2004) 167–184
- [12] Hasuo, I., Jacobs, B., Sokolova, A.: Generic trace semantics via coinduction. *Logical Methods in Computer Science* **3**(4:11) (2007) 1–36
- [13] Klin, B.: Bialgebraic methods and modal logic in structural operational semantics. *Inf. Comput.* **207**(2) (2009) 237–257
- [14] Aczel, P.: Final universes of processes. In Brookes, S., Main, M., Melton, A., Mislove, M., Schmidt, D., eds.: *Proc. 9th International Conference on Mathematical Foundations of Programming Semantics*. Volume 802 of *Lecture Notes in Computer Science*, Springer (1994) 1–28
- [15] Wolter, U.: CSP, partial automata, and coalgebras. *Theoretical Computer Science* **280** (2002) 3–34
- [16] Groote, J.F., Vaandrager, F.W.: Structural operational semantics and bisimulations as a congruence. *Information and Computation* **100**(2) (1992) 202–260
- [17] Brookes, S., Hoare, C., Roscoe, A.: A theory of communicating sequential processes. *Journal of the ACM* **31**(3) (1984) 560–599
- [18] Roggenbach, M.: CSP-CASL—A new integration of process algebra and algebraic specification. *Theoretical Computer Science* **354** (2006) 42–71