

A Coinductive Version of Milner’s Proof System for Regular Expressions Modulo Bisimilarity

Clemens Grabmayer  

Gran Sasso Science Institute, L’Aquila, Italy

Abstract

By adapting Salomaa’s complete proof system for equality of regular expressions under the language semantics, Milner (1984) formulated a sound proof system for bisimilarity of regular expressions under the process interpretation he introduced. He asked whether this system is complete. Proof-theoretic arguments attempting to show completeness of this equational system are complicated by the presence of a non-algebraic rule for solving fixed-point equations by using star iteration.

We characterize the derivational power that the fixed-point rule adds to the purely equational part Mil^- of Milner’s system Mil : it corresponds to the power of coinductive proofs over Mil^- that have the form of finite process graphs with the loop existence and elimination property LEE. We define a variant system cMil by replacing the fixed-point rule in Mil with a rule that permits LEE-shaped circular derivations in Mil^- from previously derived equations as a premise. With this rule alone we also define the variant system CLC for combining LEE-shaped coinductive proofs over Mil^- . We show that both cMil and CLC have proof interpretations in Mil , and vice versa. As this correspondence links, in both directions, derivability in Mil with derivation trees of process graphs, it widens the space for graph-based approaches to finding a completeness proof of Milner’s system.

2012 ACM Subject Classification Theory of computation \rightarrow Process calculi

Keywords and phrases regular expressions, process theory, bisimilarity, coinduction, proof theory

Digital Object Identifier 10.4230/LIPIcs.CALCO.2021.16

Related Version The report version [9] contains an extended appendix, which includes the detailed justification of the proof transformation from the coinductive system cMil to Milner’s system Mil .

Extended Version: <https://arxiv.org/abs/2108.13104>

Funding The completion of this research was supported by the PRIN project IT MATTERS – *Methods and Tools for Trustworthy Smart Systems* (with project ID: 2017FTXR7S_005).

Acknowledgements I want to thank Luca Aceto for his comments on the introduction. I am also very grateful to the anonymous reviewers for their careful reading, for spotting distracting oversights, and for asking for additional clarifications, such as concerning the motivation of coinductive proofs.

1 Introduction

Milner [13] (1984) defined a process semantics for regular expressions as process graphs: the interpretation of 0 is deadlock, of 1 is successful termination, letters a are atomic actions, the operators $+$ and \cdot stand for choice and concatenation of processes, and (unary) Kleene star $(\cdot)^*$ represents iteration with the option to terminate successfully before each execution of the iteration body. To disambiguate the use of regular expressions for denoting processes and comparing them via bisimilarity, Milner called them “star expressions”. Using bisimilarity to identify processes with the same behavior, he was interested in an axiomatization of equality of “star behaviors”, which are bisimilarity equivalence classes of star-expression processes. He adapted Salomaa’s complete proof system [14] for language equivalence on regular expressions to a system Mil that is sound for equality of denoted star behaviors. He left completeness as a question, because he recognized that Salomaa’s proof route cannot be followed directly.

Specifically, Milner gave an example showing that systems of guarded equations with star expressions cannot be solved by star expressions in general. Even if such a system is solvable, the absence from Mil of the *left*-distributivity law $x \cdot (y + z) = x \cdot y + x \cdot z$ in Salomaa’s system



© Clemens Grabmayer;

licensed under Creative Commons License CC-BY 4.0

9th Conference on Algebra and Coalgebra in Computer Science (CALCO 2021).

Editors: Fabio Gadducci and Alexandra Silva; Article No. 16; pp. 16:1–16:23

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

(it is not sound under bisimilarity) frequently prevents applications of the fixed-point rule RSP^* in Mil like in an extraction procedure from Salomaa's proof. But if RSP^* is replaced in Mil by a general unique-solvability rule scheme for guarded systems of equations (see Def. 2.4), then a complete system arises (noted in [6]). Therefore completeness of Mil hinges on whether the fixed-point rule RSP^* enables to prove equal any two star-expression solutions of a given guarded system of equations, on the basis of the purely equational part Mil^- of Mil.

As a stepping stone for tackling this difficult question, we here characterize the derivational power that the fixed-point rule RSP^* adds to the subsystem Mil^- of Mil. We do so by means of "coinductive proofs" whose shapes have the "loop existence and elimination property" LEE from [11]. This property stems from the interpretation of (1-free) star expressions, which is defined by induction on syntax trees, creating a hierarchy of "loop subgraphs". Crucially for our purpose, guarded systems of equations that correspond to finite process graphs with LEE are uniquely solvable modulo provability in Mil^- . The reason is that process graphs with LEE, which need not be in the image of the process interpretation, are amenable to applying *right*-distributivity and the rule RSP^* for an extraction procedure like in Salomaa's proof (see Section 5). These graphs can be expressed modulo bisimilarity by some star expression, which can be used to show that any two solutions modulo Mil^- of a specification of LEE-shape are Mil-provably equal. This is a crucial step in the completeness proof by Fokkink and myself in [11] for the tailored restriction BBP of Milner's system Mil to "1-free" star expressions.

Thus motivated, we define a "LLEE-witnessed coinductive proof" as a process graph \mathcal{G} with "layered" LEE (LLEE) whose vertices are labeled by equations between star expressions. The left- and the right-hand sides of the equations have to form a solution vector of a specification corresponding to the process graph \mathcal{G} . However, that specification needs to be satisfied only up to provability in Mil^- from sound assumptions. Such coinductive derivations are typically circular, like the one below of the semantically valid equation $(a + b)^* \cdot 0 = (a \cdot (a + b) + b)^* \cdot 0$:

$$(1 \cdot g^*) \cdot 0 = ((1 \cdot (a + b)) \cdot h^*) \cdot 0 \xrightarrow{a, b} (1 \cdot g^*) \cdot 0 = (1 \cdot h^*) \cdot 0$$

The process graph \mathcal{G} , which is given together with a labeling $\hat{\mathcal{G}}$ that is a "LLEE-witness" of \mathcal{G} (the colored transitions with marking labels $[n]$, for $n \in \mathbb{N}^+$, indicate LLEE-structure, see Section 3), underlies the coinductive proof on the left (see Ex. A.1 in the Appendix for a justification). \mathcal{G} is a "1-chart" that is, a process graph with 1-transitions that represent empty step processes. We depict 1-transitions as dotted arrows. For 1-charts, "1-bisimulation" is the adequate concept of bisimulation. We showed in [10, 8] that the process (chart) interpretation $\mathcal{C}(e)$ of a star expression e is the image of a 1-chart $\underline{\mathcal{C}}(e)$ with LLEE under a functional 1-bisimulation. In this example, $\mathcal{G} = \underline{\mathcal{C}}(h^* \cdot 0)$ maps by a functional 1-bisimulation to interpretations of both expressions in the conclusion. The correctness conditions for such coinductive proofs are formed by the requirement that the left-, and respectively, the right-hand sides of formal equations form "Mil $^-$ -provable solutions" of the underlying process graph: an expression at a vertex v can be reconstructed, provably in Mil^- , from the transitions to, and the expressions at, immediate successor vertices of v . Crucially we establish in Section 5, by a generalization of arguments in [11, 12] using RSP^* , that every LLEE-witnessed coinductive proof over Mil^- can be transformed into a derivation in Mil with the same conclusion.

$$\begin{array}{c}
\frac{\overbrace{(a+b)^* \cdot 0}^{e_0^*} = \overbrace{(a \cdot (a+b) + b)}^f \cdot \overbrace{(a+b)^* \cdot 0}^{e_0^*} + 0}{(a+b)^* \cdot 0 = (a \cdot (a+b) + b)^* \cdot 0} \iota, \text{RSP}^* \frac{e_0^* \cdot 0 = f \cdot (e_0^* \cdot 0) + 0}{e_0^* \cdot 0 = f^* \cdot 0} \\
(1 \cdot (a+b)) \cdot (e_0^* \cdot 0) = ((1 \cdot (a+b)) \cdot f^*) \cdot 0 \xrightarrow{a, b} 1 \cdot (e_0^* \cdot 0) = (1 \cdot f^*) \cdot 0 \\
\hat{\mathcal{C}}(f^* \cdot 0) \xleftarrow[a]{[1]} \underbrace{e_0^* \cdot 0}_{f^*} = \underbrace{(a \cdot (a+b) + b)^* \cdot 0}_{f^*} \xrightarrow[b]{[1]} 1 \\
\text{(by the premise of } \iota \text{)} \quad (a \cdot (a+b) + b) \cdot (e_0^* \cdot 0) + 0 \equiv f \cdot (e_0^* \cdot 0) + 0 =
\end{array}$$

■ **Figure 1** Mimicking an instance ι of the fixed-point rule RSP^* (above) in Milner’s system $\text{Mil} = \text{Mil}^- + \text{RSP}^*$ by a coinductive proof (below) over $\text{Mil}^- + \{\text{premise of } \iota\}$ with LLEE-witness $\hat{\mathcal{C}}(f^* \cdot 0)$. We use different colors for indicating the expressions $e_0^* \cdot 0$, f , f^* , and 0 in the instance ι of RSP^* .

This raises the question of whether the fixed-point rule RSP^* of Mil adds any derivational power to Mil^- that goes beyond those of LLEE-witnessed coinductive proofs over Mil^- , and if so, how far precisely. As our main result we show in Section 6 that every instance of the fixed-point rule RSP^* can be mimicked by a LLEE-witnessed coinductive proof over Mil^- in which also the premise of the rule may be used. It follows that the derivational power that RSP^* adds to Mil^- within Mil consists of iterating such LLEE-witnessed coinductive proofs along finite (meta-)prooftrees. The example in Fig. 1 (see Ex. A.2 in the Appendix for a justification) can give a first impression of the construction that we will use (in the proof of Lem. 6.2) to mimic instances of RSP^* . Here this construction results in a coinductive proof that only differs slightly from the one with the same underlying LLEE-1-chart we saw earlier.

Based on these two proof transformations we obtain a theorem-equivalent, coinductive variant cMil of Mil by replacing RSP^* with a rule that as one premise permits a LLEE-witnessed coinductive proof over Mil^- plus the equations of other premises. We also define a theorem-equivalent system CLC (“combining LLEE-witnessed coinductive proofs”) with this rule alone. While CLC only has LEE-shaped coinductive proofs over Mil^- as formulas, we use a hybrid concept of formula in cMil that also permits equations between star expressions.

Additionally, we formulate proof systems $\overline{\text{cMil}}$ and CC that arise from cMil and CLC by dropping “LLEE-witnessed” as a requirement for coinductive proofs. These systems are (obviously) complete for bisimilarity of process interpretations, because they can mimic the unique solvability rule scheme for guarded systems of specifications mentioned before.

Our transformations are inspired by proof-theoretic interpretations in [4] between proof systems for recursive type equality by Amadio and Cardelli [1], and by Brandt and Henglein [3]. The transformation from cMil back to Mil is similar in kind to one we described in [5] from derivations in a coinductively motivated proof system for language equivalence between regular expressions to derivations in Salomaa’s system [14] with a fixed-point rule similar to RSP^* .

2 Process semantics for star expressions, and Milner’s proof system

Here we fix terminology concerning star expressions, 1-charts, 1-bisimulations, we exhibit Milner’s system (and a few variants), and recall the chart interpretation of star expressions.

Let A be a set of *actions*. The set $\text{StExp}(A)$ of *star expressions over actions in A* are strings that are defined by the following grammar:

$$e, e_1, e_2 ::= 0 \mid 1 \mid a \mid (e_1 + e_2) \mid (e_1 \cdot e_2) \mid (e^*) \quad (\text{where } a \in A)$$

We will drop outermost brackets. We use e, f, g, h , possibly indexed and/or decorated, as syntactical variables for star expressions. We write \equiv for syntactic equality between star

expressions denoted by such syntactical variables, and values of star expression functions, in a given context, but we permit $=$ in formal equations between star expressions. We denote by $Eq(A)$ the set of formal equations $e = f$ between two star expressions $e, f \in StExp(A)$.

We define sum expressions $\sum_{i=1}^n e_i$ inductively as 0 if $n = 0$, as e_1 if $n = 1$, and as $(\sum_{i=1}^{n-1} e_i) + e_n$ if $n > 0$, for $n \in \mathbb{N} = \{0, 1, 2, \dots\}$. The (*syntactic*) *star height* $|e|_*$ of a star expression $e \in StExp(A)$ is the maximal nesting depth of stars in e , defined inductively by: $|0|_* := |1|_* := |a|_* := 0$, $|e_1 + e_2|_* := |e_1 \cdot e_2|_* := \max\{|e_1|_*, |e_2|_*\}$, and $|e^*|_* := 1 + |e|_*$.

A **1-chart** is a 6-tuple $\langle V, A, \mathbf{1}, v_s, \rightarrow, \downarrow \rangle$ where V is a finite set of *vertices*, A is a set of (*proper*) *action labels*, $\mathbf{1} \notin A$ is the specified *empty step label*, $v_s \in V$ is the *start vertex* (hence $V \neq \emptyset$), $\rightarrow \subseteq V \times A(\mathbf{1}) \times V$ is the *labeled transition relation*, where $A(\mathbf{1}) := A \cup \{\mathbf{1}\}$ is the set of action labels including $\mathbf{1}$, and $\downarrow \subseteq V$ is a set of *vertices with immediate termination*. In such a **1-chart**, we call a transition in $\rightarrow \cap (V \times A \times V)$ (labeled by a *proper action* in A) a *proper transition*, and a transition in $\rightarrow \cap (V \times \{\mathbf{1}\} \times V)$ (labeled by the *empty-step symbol* $\mathbf{1}$) a *1-transition*. Reserving non-underlined action labels like a, b, \dots for proper actions, we use underlined action label symbols like \underline{a} for actions labels in the set $A(\mathbf{1})$ that includes the label $\mathbf{1}$. We highlight in red transition labels that may involve $\mathbf{1}$.

We say that a **1-chart** is *weakly guarded* if it does not contain cycles of **1-transitions**. By a *chart* we mean a **1-chart** that is **1-free** in the sense that it does not contain **1-transitions**.

Below we define the process semantics of regular (star) expressions as (**1-free**) charts, and hence as finite, rooted labeled transition systems, which will be compared with (**1**-)bisimilarity. The charts obtained correspond to non-deterministic finite-state automata that are obtained by iterating partial derivatives [2] of Antimirov (who did not aim at a process semantics).

► **Definition 2.1.** The *chart interpretation* of a star expression $e \in StExp(A)$ is the **1-transition free chart** $\mathcal{C}(e) = \langle V(e), A, \mathbf{1}, e, \rightarrow \cap V(e), \downarrow \cap V(e) \rangle$, where $V(e)$ consists of all star expressions that are reachable from e via the labeled transition relation $\rightarrow \subseteq StExp(A) \times A \times StExp(A)$ that is defined, together with the immediate-termination relation $\downarrow \subseteq StExp(A)$, via derivability in the transition system specification (TSS) $\mathcal{T}(A)$, for $a \in A$, $e, e_1, e_2, e', e'_1, e'_2 \in StExp(A)$:

$$\frac{}{a \xrightarrow{a} \mathbf{1}} \quad \frac{e_i \xrightarrow{a} e'_i}{e_1 + e_2 \xrightarrow{a} e'_i} \quad \frac{e_1 \xrightarrow{a} e'_1}{e_1 \cdot e_2 \xrightarrow{a} e'_1 \cdot e_2} \quad \frac{e_1 \downarrow \quad e_2 \xrightarrow{a} e'_2}{e_1 \cdot e_2 \xrightarrow{a} e'_2} \quad \frac{e \xrightarrow{a} e'}{e^* \xrightarrow{a} e' \cdot e^*}$$

$$\frac{}{\mathbf{1} \downarrow} \quad \frac{e_i \downarrow}{(e_1 + e_2) \downarrow} \quad \frac{e_1 \downarrow \quad e_2 \downarrow}{(e_1 \cdot e_2) \downarrow} \quad \frac{}{(e^*) \downarrow}$$

If $e \xrightarrow{a} e'$ is derivable in $\mathcal{T}(A)$, for $e, e' \in StExp(A)$, $a \in A$, then we say that e' is a *derivative* of e . If $e \downarrow$ is derivable in $\mathcal{T}(A)$, then we say that e *permits immediate termination*.

In Section 3 we define a refinement of this interpretation from [10] into a **1-chart** interpretation. In both versions, (**1**-)charts obtained will be compared with respect to **1-bisimilarity** that relates the behavior of “induced transitions” of **1-charts**. By an *induced a-transition* $v \xrightarrow{\underline{a}} w$, for a proper action $a \in A$, in a **1-chart** \mathcal{C} we mean a path $v \xrightarrow{\mathbf{1}} \dots \xrightarrow{\mathbf{1}} \cdot \xrightarrow{a} w$ in \mathcal{C} that consists of a finite number of **1-transitions** that ends with a proper a -transition. By *induced termination* $v \downarrow^{(\mathbf{1})}$, for $v \in V$ we mean that there is a path $v \xrightarrow{\mathbf{1}} \dots \xrightarrow{\mathbf{1}} \tilde{v}$ with $\tilde{v} \downarrow$ in \mathcal{C} .

► **Definition 2.2 (1-bisimulation).** Let $\mathcal{C}_i = \langle V_i, A, \mathbf{1}, v_{s,i}, \rightarrow_i, \downarrow_i \rangle$ be **1-charts**, for $i \in \{1, 2\}$.

By a **1-bisimulation between** \mathcal{C}_1 and \mathcal{C}_2 we mean a binary relation $B \subseteq V_1 \times V_2$ such that $\langle v_{s,1}, v_{s,2} \rangle \in B$, and for every $\langle v_1, v_2 \rangle \in B$ the following three conditions hold:

- (forth) $\forall v'_1 \in V_1 \forall a \in A (v_1 \xrightarrow{\underline{a}}_1 v'_1 \implies \exists v'_2 \in V_2 (v_2 \xrightarrow{\underline{a}}_2 v'_2 \wedge \langle v'_1, v'_2 \rangle \in B))$,
- (back) $\forall v'_2 \in V_2 \forall a \in A (\exists v'_1 \in V_1 (v_1 \xrightarrow{\underline{a}}_1 v'_1 \wedge \langle v'_1, v'_2 \rangle \in B) \iff v_2 \xrightarrow{\underline{a}}_2 v'_2)$,
- (termination) $v_1 \downarrow_1^{(\mathbf{1})} \iff v_2 \downarrow_2^{(\mathbf{1})}$.

We denote by $\mathcal{C}_1 \stackrel{(\mathbf{1})}{\iff} \mathcal{C}_2$, and say that \mathcal{C}_1 and \mathcal{C}_2 are **1-bisimilar**, if there is a **1-bisimulation** between \mathcal{C}_1 and \mathcal{C}_2 . We call **1-bisimilar** (**1-free**) charts \mathcal{C}_1 and \mathcal{C}_2 *bisimilar*, and write $\mathcal{C}_1 \iff \mathcal{C}_2$.

Let A be a set. The *basic proof system* $\mathcal{EL}(A)$ of *equational logic* for star expressions has as *formulas* the formal equations between star expressions in $Eq(A)$, and the following *rules*:

$$\frac{}{e = e} \text{Refl} \quad \frac{e = f}{f = e} \text{Symm} \quad \frac{e = f \quad f = g}{e = g} \text{Trans} \quad \frac{e = f}{C[e] = C[f]} \text{Cxt}$$

that is, the rules Refl (for reflexivity), and the rules Symm (for symmetry), Trans (for transitivity), and Cxt (for filling a context), where $C[\]$ is a 1-hole star expression context.

By an \mathcal{EL} -based *system over* $StExp(A)$ (and *for star expressions over* A) we mean a proof system whose formulas are the formal equations in $Eq(A)$, and whose rules include the rules of the basic system $\mathcal{EL}(A)$ of equational logic (additionally, it may specify an arbitrary set of axioms). We will use \mathcal{S} as syntactical variable for \mathcal{EL} -based proof systems.

Let \mathcal{S} be an \mathcal{EL} -based proof system over $StExp(A)$, and $e_1, e_2 \in StExp(A)$. We permit to write $e_1 =_{\mathcal{S}} e_2$ for $\vdash_{\mathcal{S}} e_1 = e_2$, that is for the statement that there is a derivation without assumptions in \mathcal{S} that has conclusion $e_1 = e_2$.

► **Definition 2.3** (sub-system, theorem equivalence, and theorem subsumption of proof systems).

Let \mathcal{S}_1 and \mathcal{S}_2 be \mathcal{EL} -based proof systems over $StExp(A)$. We say that \mathcal{S}_1 is a *sub-system* of \mathcal{S}_2 , denoted by $\mathcal{S}_1 \subseteq \mathcal{S}_2$, if every axiom of \mathcal{S}_1 is an axiom of \mathcal{S}_2 , and every rule of \mathcal{S}_1 is also a rule of \mathcal{S}_2 . We say that \mathcal{S}_1 is *theorem-subsumed by* \mathcal{S}_2 , denoted by $\mathcal{S}_1 \lesssim \mathcal{S}_2$, if whenever a formal equation $e_1 = e_2$ is derivable in \mathcal{S}_1 (without assumptions, by using only the rules and axioms of \mathcal{S}_1), then $e_1 = e_2$ is also derivable in \mathcal{S}_2 . We say that \mathcal{S}_1 and \mathcal{S}_2 are *theorem-equivalent*, denoted by $\mathcal{S}_1 \sim \mathcal{S}_2$, if they have the same derivable equations.

► **Definition 2.4** (Milner's system Mil, variants and subsystems). Let A be a set of actions.

By the proof system $Mil^-(A)$ we mean the \mathcal{EL} -based proof system for star expressions over A with the following *axiom schemes*:

$$\begin{array}{ll} (\text{assoc}(+)) & (e + f) + g = e + (f + g) & (\text{id}_l(\cdot)) & 1 \cdot e = e \\ (\text{neutr}(+)) & e + 0 = e & (\text{id}_r(\cdot)) & e \cdot 1 = e \\ (\text{comm}(+)) & e + f = f + e & (\text{deadlock}) & 0 \cdot e = 0 \\ (\text{idempot}(+)) & e + e = e & (\text{rec}(*)) & e^* = 1 + e \cdot e^* \\ (\text{assoc}(\cdot)) & (e \cdot f) \cdot g = e \cdot (f \cdot g) & (\text{trm-body}(*)) & e^* = (1 + e)^* \\ (\text{r-distr}(+, \cdot)) & (e + f) \cdot g = e \cdot g + f \cdot g & & \end{array}$$

where $e, f, g \in StExp(A)$, and with the *rules* of the system $\mathcal{EL}(A)$ of equational logic.

The *recursive specification principle for star iteration* RSP^* , the *unique solvability principle for star iteration* USP^* , and the *general unique solvability principle* USP are the rules:

$$\frac{e = f \cdot e + g}{e = f^* \cdot g} RSP^* \text{ (if } f \downarrow) \quad \frac{e_1 = f^* \cdot e_1 + g \quad e_2 = f^* \cdot e_2 + g}{e_1 = e_2} USP^* \text{ (if } f \downarrow)$$

$$\frac{\left\{ e_{i,1} = \left(\sum_{j=1}^{n_i} f_{i,j} \cdot e_{j,1} \right) + g_i \quad e_{i,2} = \left(\sum_{j=1}^{n_i} f_{i,j} \cdot e_{j,2} \right) + g_i \right\}_{i=1,\dots,n}}{e_{1,1} = e_{1,2}} USP \text{ (if } f_{i,j} \downarrow \text{ for all } i, j)$$

Milner's proof system $Mil(A)$ is the extension of $Mil^-(A)$ by adding the rule RSP^* . Its variant systems $Mil'(A)$, and $\bar{M}il'(A)$, arise from $Mil^-(A)$ by adding (instead of RSP^*) the rule USP^* , and respectively, the rule USP . $ACI(A)$ is the system with the axioms for associativity, commutativity, and idempotency for $+$. We will keep the action set A implicit in the notation.

► **Proposition 2.5** (Milner, [13]). *Mil is sound for bisimilarity of chart interpretations. That is, for all $e, f \in StExp(A)$ it holds: $(e =_{Mil} f \implies \mathcal{C}(e) \Leftrightarrow \mathcal{C}(f))$.*

► **Question 2.6** (Milner, [13]). Is Mil also complete for bisimilarity of process interpretations? That is, does for all $e, f \in StExp(A)$ the implication $(e =_{Mil} f \iff \mathcal{C}(e) \leftrightarrow \mathcal{C}(f))$ hold?

► **Definition 2.7** (provable solutions). Let \mathcal{S} be an \mathcal{EL} -based proof system for star expressions over A that extends ACI. Let $\underline{\mathcal{C}} = \langle V, A, \mathbf{1}, v_s, \rightarrow, \downarrow \rangle$ be a **1-chart**.

By a *star expression function on $\underline{\mathcal{C}}$* we mean a function $s : V \rightarrow StExp(A)$ on the vertices of $\underline{\mathcal{C}}$. Let $v \in V$. We say that such a star expression function s on $\underline{\mathcal{C}}$ is an *\mathcal{S} -provable solution of $\underline{\mathcal{C}}$ at v* if it holds that $s(v) =_{\mathcal{S}} \tau_{\underline{\mathcal{C}}}(v) + \sum_{i=1}^n a_i \cdot s(v_i)$, given the (possibly redundant) list representation $T_{\underline{\mathcal{C}}}(v) = \{v \xrightarrow{a_i} v_i \mid i \in \{1, \dots, n\}\}$, of transitions from v in $\underline{\mathcal{C}}$ and where $\tau_{\underline{\mathcal{C}}}(v)$ is the *termination constant $\tau_{\underline{\mathcal{C}}}(v)$ of $\underline{\mathcal{C}}$ at v* defined as 0 if $v \not\downarrow$, and as 1 if $v \downarrow$. This definition does not depend on the specifically chosen list representation of $T_{\underline{\mathcal{C}}}(v)$, because \mathcal{S} extends ACI, and therefore it contains the associativity, commutativity, and idempotency axioms for $+$.

By an *\mathcal{S} -provable solution of $\underline{\mathcal{C}}$* (with *principal value $s(v_s)$ at the start vertex v_s*) we mean a star expression function s on $\underline{\mathcal{C}}$ that is an \mathcal{S} -provable solution of $\underline{\mathcal{C}}$ at every vertex of $\underline{\mathcal{C}}$.

3 Layered loop existence and elimination, and LLEE-witnesses

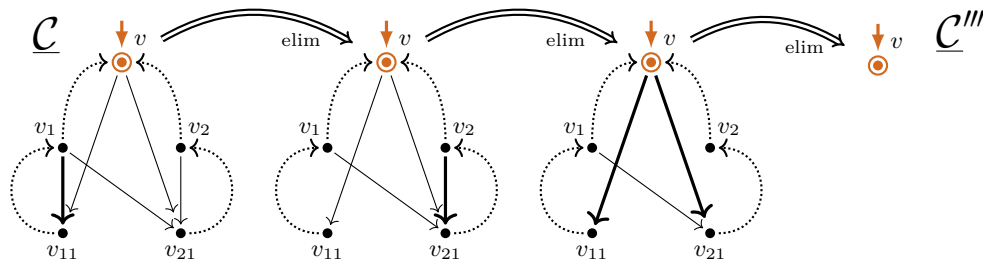
In this subsection we briefly recall principal definitions and statements from [11, 10]. We keep formalities to a minimum as necessary for our purpose (in particular for “LLEE-witnesses”).

A **1-chart** $\underline{\mathcal{C}} = \langle V, A, \mathbf{1}, v_s, \rightarrow, \downarrow \rangle$ is called a *loop 1-chart* if it satisfies three conditions:

- (L1) There is an infinite path from the start vertex v_s .
- (L2) Every infinite path from v_s returns to v_s after a positive number of transitions.
- (L3) Immediate termination is only permitted at the start vertex, that is, $\downarrow \subseteq \{v_s\}$.

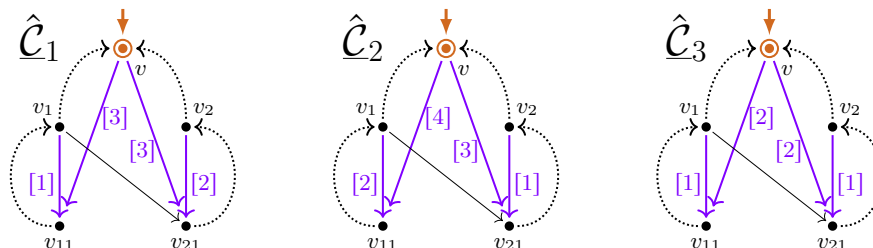
We call the transitions from v_s *loop-entry transitions*, and all other transitions *loop-body transitions*. A *loop sub-1-chart* of a **1-chart** $\underline{\mathcal{C}}$ is a loop **1-chart** $\underline{\mathcal{L}}$ that is a sub-**1-chart** of $\underline{\mathcal{C}}$ with some vertex $v \in V$ of $\underline{\mathcal{C}}$ as start vertex, such that $\underline{\mathcal{L}}$ is constructed, for a nonempty set U of transitions of $\underline{\mathcal{C}}$ from v , by all paths that start with a transition in U and continue onward until v is reached again (so the transitions in U are the loop-entry transitions of $\underline{\mathcal{L}}$).

The result of *eliminating a loop sub-1-chart $\underline{\mathcal{L}}$ from a **1-chart** $\underline{\mathcal{C}}$* arises by removing loop-entry transitions of $\underline{\mathcal{L}}$ from $\underline{\mathcal{C}}$, and then also removing all vertices and transitions that become unreachable. We say that a **1-chart** $\underline{\mathcal{C}}$ has the *loop existence and elimination property* (LEE) if the procedure, started on $\underline{\mathcal{C}}$, of repeated eliminations of loop sub-**1-charts** results in a **1-chart** without an infinite path. If, in a successful elimination process from a **1-chart** $\underline{\mathcal{C}}$, loop-entry transitions are never removed from the body of a previously eliminated loop sub-**1-chart**, then we say that $\underline{\mathcal{C}}$ satisfies *layered LEE* (LLEE), and is a *LLEE-1-chart*. While the property LLEE leads to a formally easier concept of “witness”, it is equivalent to LEE. (For an example of a LEE-witness that is not layered, see further below on page 7.)



The picture above shows a successful run of the loop elimination procedure. In brown we highlight start vertices by \rightarrow , and immediate termination with a boldface ring by \odot . The loop-entry transitions of loop sub-**1-charts** that are eliminated in the next step are marked in bold.

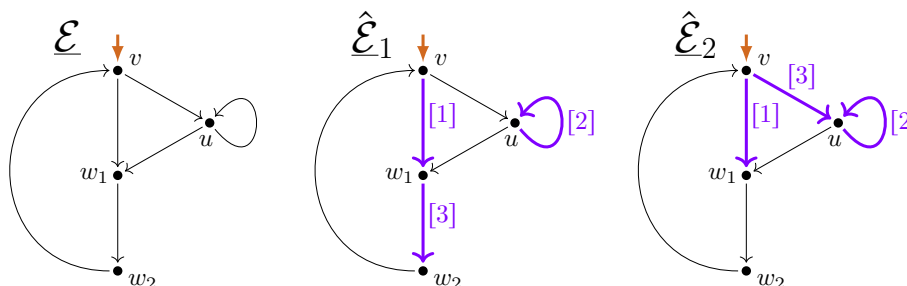
We have neglected action labels here, except for indicating 1-transitions by dotted arrows. Since the graph $\underline{\mathcal{C}}'''$ that is reached after three loop-subgraph elimination steps from the 1-chart $\underline{\mathcal{C}}$ does not have an infinite path, and no loop-entry transitions have been removed from a previously eliminated loop sub-1-chart, we conclude that $\underline{\mathcal{C}}$ satisfies LEE and LLEE.



A LLEE-witness $\hat{\mathcal{C}}$ of a 1-chart $\underline{\mathcal{C}}$ is the recording of a successful run of the loop elimination procedure by attaching to a transition τ of $\underline{\mathcal{C}}$ the marking label n for $n \in \mathbb{N}^+$ (in pictures indicated as $[n]$, in steps as $\rightarrow_{[n]}$) forming a *loop-entry transition* if τ is eliminated in the n -th step, and by attaching marking label 0 to all other transitions of $\underline{\mathcal{C}}$ (in pictures neglected, in steps indicated as \rightarrow_{bo}) forming a *body transition*. Formally, LLEE-witnesses arise as *entry/body-labelings* from 1-charts, and are charts in which the transition labels are pairs of action labels over A , and marking labels in \mathbb{N} . We say that a LLEE-witness $\hat{\mathcal{C}}$ is *guarded* if all loop-entry transitions are proper, which means that they have a proper-action transition label.

The entry/body-labeling $\hat{\mathcal{C}}_1$ above of the 1-chart $\underline{\mathcal{C}}$ is a LLEE-witness that arises from the run of the loop elimination procedure earlier above. The entry/body-labelings $\hat{\mathcal{C}}_2$ and $\hat{\mathcal{C}}_3$ of $\underline{\mathcal{C}}$ record two other successful runs of the loop elimination procedure of length 4 and 2, respectively, where for $\hat{\mathcal{C}}_3$ we have permitted to eliminate two loop subcharts at different vertices together in the first step. The 1-chart $\underline{\mathcal{C}}$ above only has layered LEE-witnesses.

The situation is different for the 1-chart $\underline{\mathcal{E}}$ below:



The entry/body-labeling $\hat{\mathcal{E}}_1$ of $\underline{\mathcal{E}}$ as above is a LEE-witness that is not layered: in the third loop sub-1-chart elimination step that is recorded in $\hat{\mathcal{E}}_1$ the loop-entry transition from w_1 to w_2 is removed, which is in the body of the loop sub-1-chart at v with loop-entry transition from v to w_1 that (by that time) has already been removed in the first loop-elimination step as recorded in $\hat{\mathcal{E}}_1$. By contrast, the entry/body-labeling $\hat{\mathcal{E}}_2$ of $\underline{\mathcal{E}}$ above is a layered LEE-witness. In general it can be shown that every LEE-witness that is not layered can be transformed into a LLEE-witness of the same underlying 1-chart. Indeed, the step from $\hat{\mathcal{E}}_1$ to $\hat{\mathcal{E}}_2$ in the example above, which transfers the loop-entry transition marking label $[3]$ from the transition from w_1 to w_2 over to the transition from v to u , hints at the proof of this statement. However, we do not need this result, because we will be able to use the guaranteed existence of LLEE-witnesses (see Thm. 3.3) for the 1-chart interpretation below (see Def. 3.2).

In a LLEE-witness we denote by $v \rightsquigarrow w$, and by $w \leftarrow v$, that w is in the body of the loop sub-1-chart at v , which means that there is a path $v \rightarrow_{[n]} v' \rightarrow_{\text{bo}}^* w$ from v via a loop-entry transition and subsequent body transitions without encountering v again.

► **Lemma 3.1.** *The relations \rightsquigarrow and \rightarrow_{bo} defined by a LLEE-witness $\hat{\mathcal{C}}$ of a 1-chart $\underline{\mathcal{C}}$ satisfy:*

- (i) \leftarrow^+ is a well-founded, strict partial order on V .
- (ii) \leftarrow_{bo}^+ is a well-founded strict partial order on V .

► **Definition 3.2** (1-chart interpretation of star expressions). By the 1-chart interpretation $\underline{\mathcal{C}}(e)$ of a star expression e we mean the 1-chart that arises together with the entry/body-labeling $\hat{\mathcal{C}}(e)$ as the e -rooted sub-LTS generated by $\{e\}$ according to the following TSS:

$$\frac{}{a \xrightarrow{\text{bo}} 1} \quad \frac{e_i \xrightarrow{l} E'_i \quad (i \in \{1, 2\})}{e_1 + e_2 \xrightarrow{\text{bo}} E'_i} \quad \frac{e \xrightarrow{l} E' \quad (\text{if } nd^+(e))}{e^* \xrightarrow{[[e^*|*]]} E' * e^*} \quad \frac{e \xrightarrow{l} E' \quad (\text{if } \neg nd^+(e))}{e^* \xrightarrow{\text{bo}} E' * e^*}$$

$$\frac{E_1 \xrightarrow{l} E'_1}{E_1 \cdot e_2 \xrightarrow{l} E'_1 \cdot e_2} \quad \frac{E_1 \xrightarrow{l} E'_1}{E_1 * e_2^* \xrightarrow{l} E'_1 * e_2^*} \quad \frac{e_1 \downarrow \quad e_2 \xrightarrow{l} E'_2}{e_1 \cdot e_2 \xrightarrow{\text{bo}} E'_2} \quad \frac{e_1 \downarrow}{e_1 * e_2^* \xrightarrow{\text{bo}} e_2^*}$$

where $l \in \{\text{bo}\} \cup \{[n] \mid n \in \mathbb{N}^+\}$, and star expressions using a “stacked” product operation $*$ are permitted, which helps to record iterations from which derivatives originate. Immediate termination for expressions of $\underline{\mathcal{C}}(e)$ is defined by the same rules as in Def. 2.1 (for star expressions only, preventing immediate termination for expressions with stacked product $*$). The condition $nd^+(e)$ means that e permits a positive length path to an expression f with $f \downarrow$. We use a projection function π that changes occurrences of stacked product $*$ into product \cdot .

► **Theorem 3.3** ([8, 10]). *For every $e \in \text{StExp}(A)$, (a) the entry/body-labeling $\hat{\mathcal{C}}(e)$ of $\underline{\mathcal{C}}(e)$ is a LLEE-witness of $\underline{\mathcal{C}}(e)$, and (b) the projection function π defines a 1-bisimulation from the 1-chart interpretation $\underline{\mathcal{C}}(e)$ of e to the chart interpretation $\mathcal{C}(e)$ of e , and hence $\underline{\mathcal{C}}(e) \stackrel{(1)}{\leftrightarrow} \mathcal{C}(e)$.*

Lem. 3.5 below follows from the next lemma, whose proof we sketch in the appendix.

► **Lemma 3.4.** $\pi(E) =_{\text{Mil}^-} \tau_{\underline{\mathcal{C}}(E)}(E) + \sum_{i=1}^n \underline{a}_i \cdot \pi(E'_i)$, given a list representation $T_{\underline{\mathcal{C}}(E)}(w) = \{E \xrightarrow{\underline{a}_i} E'_i \mid i \in \{1, \dots, n\}\}$ of the transitions from E in $\underline{\mathcal{C}}(E)$.

► **Lemma 3.5.** *For every star expression $e \in \text{StExp}(A)$ with 1-chart interpretation $\underline{\mathcal{C}}(e) = \langle V(e), A, \mathbf{1}, e, \rightarrow, \downarrow \rangle$ the star-expression function $s : V(e) \rightarrow \text{StExp}(A)$, $E \mapsto \pi(E)$ is a Mil^- -provable solution of $\underline{\mathcal{C}}(e)$ with principal value e .*

4 Coinductive version of Milner's proof system

In this section we motivate and define “coinductive proofs”, introduce coinductive versions of Milner's system Mil , and establish first interconnections between these proof systems.

A finite 1-bisimulation between the 1-chart interpretations of star expressions e_1 and e_2 can be viewed as a proof of the statement that e_1 and e_2 define the same star behavior. This can be generalized by permitting finite 1-bisimulations up to provability in Mil , that is, finite relations B on star expressions for which pairs $\langle v_1, v_2 \rangle \in B$ progress, via the (forth) and (back) conditions in Def. 2.2, to pairs $\langle v'_1, v'_2 \rangle$ in the (infinite) composed relation $=_{\text{Mil}} \cdot B \cdot =_{\text{Mil}}$. Now 1-bisimilarity up to $=_{\text{Mil}}$ entails 1-bisimilarity of the 1-chart interpretations, and bisimilarity of chart interpretations, due to soundness of Mil (see Prop. 2.5). In order to link, later in Section 5, coinductive proofs with proofs in Milner's system Mil , we will be interested in 1-bisimulations up to $=_{\mathcal{S}}$ for systems \mathcal{S} with $\text{ACI} \subseteq \mathcal{S} \lesssim \text{Mil}$ that have the form of LLEE-1-charts, which will guarantee such a connection. First we introduce a “LLEE-witnessed coinductive proof” as an equation-labeled, LLEE-1-chart $\underline{\mathcal{C}}$ that defines a 1-bisimulation up to $=_{\mathcal{S}}$ for \mathcal{S} with $\text{ACI} \subseteq \mathcal{S}$ from the left-/right-hand sides of equations on the vertices of $\underline{\mathcal{C}}$ (see Rem. 4.4).

► **Definition 4.1** ((LLEE-witnessed) coinductive proofs). Let $e_1, e_2 \in \text{StExp}(A)$ be star expressions, and let \mathcal{S} be an \mathcal{EL} -based proof system for star expressions over A with $\text{ACI} \subseteq \mathcal{S}$.

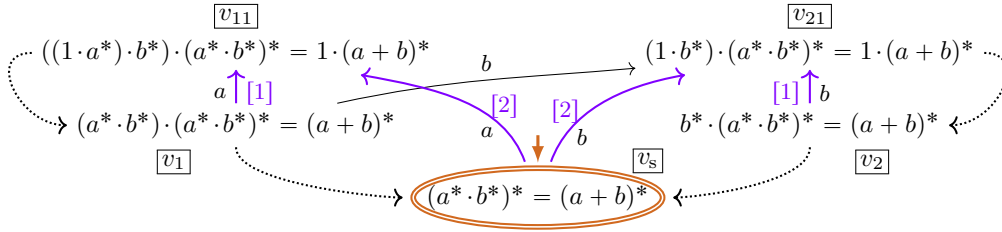
A *coinductive proof over \mathcal{S} of $e_1 = e_2$* is a pair $\mathcal{CP} = \langle \underline{\mathcal{C}}, L \rangle$ where $\underline{\mathcal{C}} = \langle V, A, \mathbf{1}, v_s, \rightarrow, \downarrow \rangle$ is a weakly guarded **1**-chart, and $L : V \rightarrow \text{Eq}(A)$ a labeling function of vertices of $\underline{\mathcal{C}}$ by formal equations over A such that for the functions $L_1, L_2 : V \rightarrow \text{StExp}(A)$ that denote the star expressions $L_1(v)$, and $L_2(v)$, on the left-, and on the right-hand side of the equation $L(v)$, respectively, the following conditions hold:

(cp1) L_1 and L_2 are \mathcal{S} -provable solutions of $\underline{\mathcal{C}}$,

(cp2) $e_1 \equiv L_1(v_s)$ and $e_2 \equiv L_2(v_s)$.

By a *LLEE-witnessed coinductive proof* we mean a coinductive proof $\mathcal{CP} = \langle \underline{\mathcal{C}}, L \rangle$ where $\underline{\mathcal{C}}$ is a LLEE-**1**-chart. We denote by $e \stackrel{\text{coind}}{=}_{\mathcal{S}} f$ that there is a coinductive proof over \mathcal{S} of $e = f$, and by $e \stackrel{\text{LLEE}}{=}_{\mathcal{S}} f$ that there is a LLEE-witnessed coinductive proof over \mathcal{S} of $e = f$.

► **Example 4.2.** The statement $(a^* \cdot b^*)^* \stackrel{\text{LLEE}}{=}_{\text{Mil}^-} (a + b)^*$ can be established by the following LLEE-witnessed coinductive proof $\mathcal{CP} = \langle \underline{\mathcal{C}}, L \rangle$ over Mil^- where $\underline{\mathcal{C}} = \underline{\mathcal{C}}((a^* \cdot b^*)^*)$ has the indicated LLEE-witness $\hat{\underline{\mathcal{C}}}((a^* \cdot b^*)^*)$ (see Thm. 3.3) where framed boxes contain vertex names:



Here we have drawn the **1**-chart $\underline{\mathcal{C}}$ that carries the equations with its start vertex below in order to adhere to the proof tree intuition for the represented derivation, namely with the conclusion at the bottom. We will do so repeatedly also below. Solution correctness conditions for the left-hand sides of the equations on $\underline{\mathcal{C}}$ follows from Lem. 3.5, due to $\underline{\mathcal{C}} = \underline{\mathcal{C}}((a^* \cdot b^*)^*)$ as $(a^* \cdot b^*)^*$ is the left-hand side of the conclusion. However, we verify the correctness conditions for the left- and the right-hand sides for the (most involved) case of vertex v_1 together as follows (we usually neglect associative brackets, and combine some axiom applications):

$$\begin{aligned}
(a^* \cdot b^*) \cdot (a^* \cdot b^*)^* &=_{\text{Mil}^-} ((1 + a \cdot a^*) \cdot (1 + b \cdot b^*)) \cdot (a^* \cdot b^*)^* \\
&=_{\text{Mil}^-} (1 \cdot 1 + a \cdot a^* \cdot 1 + 1 \cdot b \cdot b^* + a \cdot a^* \cdot b \cdot b^*) \cdot (a^* \cdot b^*)^* \\
&=_{\text{Mil}^-} (1 + a \cdot a^* + a \cdot a^* \cdot b \cdot b^* + b \cdot b^*) \cdot (a^* \cdot b^*)^* \\
&=_{\text{Mil}^-} (1 + a \cdot a^* \cdot (1 + b \cdot b^*) + b \cdot b^*) \cdot (a^* \cdot b^*)^* \\
&=_{\text{Mil}^-} (1 + a \cdot a^* \cdot b^* + b \cdot b^*) \cdot (a^* \cdot b^*)^* \\
&=_{\text{Mil}^-} 1 \cdot (a^* \cdot b^*)^* + a \cdot (((1 \cdot a^*) \cdot b^*) \cdot (a^* \cdot b^*)^*) + b \cdot ((1 \cdot b^*) \cdot (a^* \cdot b^*)^*) \\
(a + b)^* &=_{\text{Mil}^-} (a + b)^* + (a + b)^* =_{\text{Mil}^-} 1 + (a + b) \cdot (a + b)^* + 1 + (a + b) \cdot (a + b)^* \\
&=_{\text{Mil}^-} 1 + 1 + (a + b) \cdot (a + b)^* + a \cdot (a + b)^* + b \cdot (a + b)^* \\
&=_{\text{Mil}^-} 1 + (a + b) \cdot (a + b)^* + a \cdot (1 \cdot (a + b)^*) + b \cdot (1 \cdot (a + b)^*) \\
&=_{\text{Mil}^-} 1 \cdot (a + b)^* + a \cdot (1 \cdot (a + b)^*) + b \cdot (1 \cdot (a + b)^*)
\end{aligned}$$

The solution conditions at the vertices v and v_2 can be verified analogously. At v_{11} and at v_{21} the solution conditions follow by uses of the axiom $\text{id}_1(\cdot)$ of Mil^- .

► **Lemma 4.3.** Let $R \in \{ \stackrel{\text{coind}}{=}_{\mathcal{S}}, \stackrel{\text{LLEE}}{=}_{\mathcal{S}} \}$ for some \mathcal{EL} -based proof system \mathcal{S} with $\text{ACI} \subseteq \mathcal{S}$. Then R is reflexive, symmetric, and satisfies $=_{\mathcal{S}} \circ R \subseteq R$, $R \circ =_{\mathcal{S}} \subseteq R$, and $=_{\mathcal{S}} \subseteq R$.

16:10 A Coinductive Version of Milner's Proof System

► **Remark 4.4.** For every coinductive proof $\mathcal{CP} = \langle \underline{\mathcal{C}}, L \rangle$, whether \mathcal{CP} is LLEE-witnessed or not, over an \mathcal{EL} -based proof system \mathcal{S} with $\text{ACI} \subseteq \mathcal{S} \lesssim \text{Mil}$ the finite relation defined by:

$$B := \left\{ \left\langle \tau_{\underline{\mathcal{C}}}(v) + \sum_{i=1}^n \underline{a}_i \cdot L_1(v_i), \tau_{\underline{\mathcal{C}}}(v) + \sum_{i=1}^n \underline{a}_i \cdot L_2(v_i) \right\rangle \mid \begin{array}{l} T_{\underline{\mathcal{C}}}(v) = \{v \xrightarrow{\underline{a}_i} v_i \mid i \in \{1, \dots, n\}\}, \\ v \in V(\underline{\mathcal{C}}), \text{ the set of vertices of } \underline{\mathcal{C}} \end{array} \right\}$$

is a bisimulation up to $=_{\mathcal{S}}$ with respect to the labeled transition system on all star expressions that is defined by the TSS in Def. 2.1. This can be shown by using that the left-hand sides $L_1(v)$, and respectively the right-hand sides $L_2(v)$, of the equations $L(v)$ in \mathcal{CP} , for $v \in V(\underline{\mathcal{C}})$, form \mathcal{S} -provable solutions of the 1-chart $\underline{\mathcal{C}}$ that underlies \mathcal{CP} .

► **Definition 4.5** (proof systems CLC, CC for combining (LLEE-witnessed) coinductive proofs). By the *proof system CLC(A) for combining LLEE-witnessed coinductive proofs (over extensions of $\text{Mil}^-(A)$) between star expressions over A* we mean the Hilbert-style proof system whose *formulas* are equations between star expressions in $\text{Eq}(A)$ or LLEE-witnessed coinductive proofs over $\text{Mil}^-(A) + \Delta$, where $\Delta \in \text{Eq}(A)$, and whose *rules* are those of the scheme:

$$\frac{g_1 = h_1 \ \dots \ g_n = h_n \quad \mathcal{LCP}_{\text{Mil}^- + \Gamma}(e = f)}{e = f} \quad \text{LCoProof}_n \quad \begin{array}{l} \text{(where } \Gamma = \{g_1 = h_1, \dots, g_n = h_n\}, \text{ and} \\ \mathcal{LCP}_{\text{Mil}^- + \Gamma}(e = f) \text{ is a LLEE-witnessed} \\ \text{coind. proof of } e = f \text{ over } \text{Mil}^- + \Gamma) \end{array}$$

where $n \in \mathbb{N}$ (including $n = 0$), and the $(n + 1)$ -th premise of an instance of LCoProof_n consists of a LLEE-witnessed coinductive proof \mathcal{CP} of $e = f$ over Mil^- plus the formulas of the other premises. By the *proof system CC(A) for combining coinductive proofs (over extensions of $\text{Mil}^-(A)$) between star expressions over A* we mean the analogous system with a rule CoProof_n whose $(n + 1)$ -th premise is a coinductive proof \mathcal{CP} of $e = f$ over $\text{Mil}^-(A)$ plus the formulas of the other premises that establishes $e \xrightarrow{\text{coind}}_{(\text{Mil}^- + \Gamma)} f$ (thus here coinductive proofs do not need to be LLEE-witnessed). Keeping A implicit, we write CLC and CC for $\text{CLC}(A)$ and $\text{CC}(A)$, respectively. Note that CLC and CC do not contain the rules of \mathcal{EL} nor any axioms; instead, derivations have to start with 0-premise instances of LCoProof_0 or CoProof_0 .

We now define a coinductively motivated variant cMil of Milner's proof system Mil . In order to obtain cMil we drop the fixed-point rule RSP^* from Mil , obtaining Mil^- , and then add a rule each of whose instances use, as a premise, an entire LLEE-witnessed coinductive proof over Mil^- and equations in other premises.

► **Definition 4.6** (proof systems cMil , cMil_1 , $\overline{\text{cMil}}$). Let A be a set of actions.

The proof system $\text{cMil}(A)$, the *coinductive variant of $\text{Mil}(A)$* , has the same *formulas* as $\text{CLC}(A)$ (formal equations and coinductive proofs), its *axioms* are those of $\text{Mil}^-(A)$, and its *rules* are those of $\mathcal{EL}(A)$, plus the *rule scheme* $\{\text{LCoProof}_n\}_{n \in \mathbb{N}}$ from $\text{CLC}(A)$. By $\text{cMil}_1(A)$ we mean the *simple coinductive variant of $\text{Mil}(A)$* , in which only the rule LCoProof_1 of $\text{CLC}(A)$ is added to the rules and axioms of $\text{Mil}^-(A)$. By $\overline{\text{cMil}}(A)$ we mean the variant of $\text{cMil}(A)$ in which the more general *rule scheme* $\{\text{CoProof}_n\}_{n \in \mathbb{N}}$ from $\text{CC}(A)$ is used instead.

We again permit to write cMil , cMil_1 , $\overline{\text{cMil}}$ for $\text{cMil}(A)$, $\text{cMil}_1(A)$, and $\overline{\text{cMil}}(A)$, respectively.

► **Lemma 4.7.** *The following theorem subsumption and equivalence statements hold:*

- (i) $\text{cMil}_1 \lesssim \text{cMil}$.
- (ii) $\text{CLC} \sim \text{cMil}$.
- (iii) $\text{CC} \sim \overline{\text{cMil}}$.

Proof. Statement (i) is due to $\text{cMil}_1 \subseteq \text{cMil}$, as cMil_1 is a subsystem of cMil that arises by restricting the rule scheme $\{\text{LCoProof}_i\}_{i \in \mathbb{N}}$ to the single rule LCoProof_1 .

For (ii), $\text{CLC} \lesssim \text{cMil}$ follows from $\text{CLC} \subseteq \text{cMil}$. For showing the converse implication, $\text{CLC} \gtrsim \text{cMil}$, it suffices to transform an arbitrary derivation in cMil into a derivation in CLC . For this purpose, all instances of axioms and rules of Mil^- have to be eliminated from derivations in cMil , keeping only instances of LCoProof_k for $k \in \mathbb{N}$. This can be done by extending the equation premises of rules LCoProof_k if required. For example, a derivation with a bottommost instance of LCoProof_1 in which the subderivation \mathcal{D} does not contain any instances of LCoProof_k for $k \in \mathbb{N}$ below the conclusions $g_1 = h_1, \dots, g_m = h_m$ of instances of $\text{LCoProof}_{k_1}, \dots, \text{LCoProof}_{k_m}$:

$$\frac{\frac{\mathcal{D}_1 \quad \dots \quad \mathcal{D}_m}{(g_1 = h_1) \dots (g_m = h_m)} \quad \mathcal{D}}{\frac{g = h \quad \mathcal{LCP}(e = f)}{e = f} \text{LCoProof}_1} \implies \frac{\frac{\mathcal{D}_1 \quad \dots \quad \mathcal{D}_m}{(g_1 = h_1) \dots (g_m = h_m)} \quad \mathcal{LCP}'(e = f)}{e = f} \text{LCoProof}_m$$

can be replaced, on the right, by a single instance of LCoProof_m , where $\mathcal{LCP}'(e = f)$ is, while formally the same as $\mathcal{LCP}(e = f)$, now a LLEE-witnessed coinductive proof over Mil^- plus $g_1 = h_1, \dots, g_m = h_m$. The latter is possible because the derivation part \mathcal{D} in Mil^- implies that then $g = h$ can be derived from the assumptions in Mil^- as well.

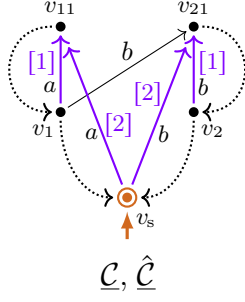
Statement (iii) can be shown entirely analogously as statement (ii). \blacktriangleleft

► **Remark 4.8** (completeness of CC , $\overline{\text{cMil}}$, $\overline{\text{Mil}'}$). The proof systems CC and $\overline{\text{cMil}}$, as well as the variant $\overline{\text{Mil}'}$ of Milner's system with the general unique solvability principle USP are complete for bisimilarity of star expressions. This can be established along Salomaa's completeness proof for his inference system for language equality of regular expressions [14], by an argument that we can outline as follows. Given star expressions e and f with $\mathcal{C}(e) \leftrightarrow \mathcal{C}(f)$, e and f can be shown to be principal values of Mil^- -provable solutions of $\mathcal{C}(e)$ and $\mathcal{C}(f)$, respectively (by a lemma for the chart interpretation similar to Lem. 3.5). These solutions can be transferred to the (1-free) product chart \mathcal{C} of $\mathcal{C}(e)$ and $\mathcal{C}(f)$, with e and f as principal values of Mil^- -provable solutions L_1 and L_2 of \mathcal{C} , respectively. From this we obtain a (not necessarily LLEE-witnessed) coinductive proof $\langle \mathcal{C}, L \rangle$ of $e = f$ over Mil^- . It follows that $e = f$ is provable in CC , and in $\overline{\text{cMil}}$. Now since the correctness conditions for the Mil^- -provable solutions L_1 and L_2 of \mathcal{C} at each of the vertices of \mathcal{C} together form a guarded system of linear equations to which the rule USP can be applied (as \mathcal{C} is 1-free), we obtain that $e = f$ is also provable in $\overline{\text{Mil}'}$.

5 From LLEE-witnessed coinductive proofs to Milner's system

In this section we show that every LLEE-witnessed coinductive proof over Mil^- of an equation can also be established by a proof in Milner's system Mil . As a consequence we show that the coinductive version cMil of Mil is theorem-subsumed by Mil . We obtain the statements in this section by adapting results in [11, 12, Sect. 5] from LLEE-charts to LLEE-1-charts.

The hierarchical loop structure of a 1-chart $\hat{\mathcal{C}}$ with LLEE-witness $\hat{\mathcal{C}}$ facilitates the extraction of a Mil^- -provable solution of $\underline{\mathcal{C}}$ (see Lem. 5.4), for the following reason. The behaviour at every vertex w in $\underline{\mathcal{C}}$ can be split into an iteration part that is induced via the loop-entry transitions from w in $\hat{\mathcal{C}}$ (which induce loop sub-1-charts with inner loop sub-1-charts whose behaviour can be synthesized recursively), and an exit part that is induced via the body transitions from w in $\hat{\mathcal{C}}$. This idea permits to define (Def. 5.1) an "extraction function" $s_{\hat{\mathcal{C}}}$ of $\hat{\mathcal{C}}$



$$\begin{aligned}
 t_{\hat{\mathcal{C}}}(v_{21}, v_2) &:= 0^* \cdot (1 \cdot t_{\hat{\mathcal{C}}}(v_2, v_2)) \equiv 0^* \cdot (1 \cdot 1) =_{\text{Mil}^-} 1 \\
 t_{\hat{\mathcal{C}}}(v_2, v_s) &:= (b \cdot t_{\hat{\mathcal{C}}}(v_{21}, v_2))^* \cdot (1 \cdot t_{\hat{\mathcal{C}}}(v_s, v_s)) =_{\text{Mil}^-} b^* \\
 t_{\hat{\mathcal{C}}}(v_{21}, v_s) &:= 0^* \cdot (1 \cdot t_{\hat{\mathcal{C}}}(v_2, v_s)) =_{\text{Mil}^-} 1 \cdot b^* =_{\text{Mil}^-} b^* \\
 t_{\hat{\mathcal{C}}}(v_{11}, v_1) &:= 0^* \cdot (1 \cdot t_{\hat{\mathcal{C}}}(v_1, v_1)) \equiv 0^* \cdot (1 \cdot 1) =_{\text{Mil}^-} 1 \\
 t_{\hat{\mathcal{C}}}(v_1, v_s) &:= (a \cdot t_{\hat{\mathcal{C}}}(v_{11}, v_s))^* \cdot (b \cdot t_{\hat{\mathcal{C}}}(v_{21}, v_s) + 1 \cdot t_{\hat{\mathcal{C}}}(v_s, v_s)) \\
 &=_{\text{Mil}^-} a^* \cdot (b \cdot b^* + 1) =_{\text{Mil}^-} a^* \cdot b^* \\
 t_{\hat{\mathcal{C}}}(v_{11}, v_s) &:= 0^* \cdot (1 \cdot t_{\hat{\mathcal{C}}}(v_1, v_s)) =_{\text{Mil}^-} a^* \cdot b^* \\
 s_{\hat{\mathcal{C}}}(v_s) &:= (a \cdot t_{\hat{\mathcal{C}}}(v_{11}, v_s) + b \cdot t_{\hat{\mathcal{C}}}(v_{21}, v_s))^* \cdot 1 \\
 &=_{\text{Mil}^-} (a \cdot (a^* \cdot b^*) + b \cdot b^*)^*
 \end{aligned}$$

■ **Figure 2** Extraction of the principal value $s_{\hat{\mathcal{C}}}(v_s)$ of a Mil^- -provable solution $s_{\hat{\mathcal{C}}}$ from the LLEE-witness $\hat{\mathcal{C}}$ used for the coinductive proof in Ex. 4.2. We shorten solution values by using axioms of Mil^- .

from a “relative extraction function” $t_{\hat{\mathcal{C}}}$ of $\hat{\mathcal{C}}$ whose values $t_{\hat{\mathcal{C}}}(w, v)$ capture the behaviour at w in a loop sub-1-chart at v until v is reached. By the same idea the fixed-point rule RSP^* can be used for showing that any two Mil -provable solutions of \mathcal{C} are Mil -provably equal (Lem. 5.6). We provide examples for these statements that hint at their proofs (Ex. 5.2, Ex. 5.8), but we refer to the extended version [9] for the detailed arguments that are similar as in [11, 12].

► **Definition 5.1** ((relative) extraction function). Let $\mathcal{C} = \langle V, A, \mathbf{1}, v_s, \rightarrow, \downarrow \rangle$ be a 1-chart with guarded LLEE-witness $\hat{\mathcal{C}}$. The *extraction function* $s_{\hat{\mathcal{C}}} : V \rightarrow \text{StExp}(A)$ of $\hat{\mathcal{C}}$ is defined from the *relative extraction function* $t_{\hat{\mathcal{C}}} : \{ \langle w, v \rangle \mid w, v \in V(\mathcal{C}), w \leftarrow^= v \}$ of $\hat{\mathcal{C}}$ as follows, for $w, v \in V$:

$$\begin{aligned}
 t_{\hat{\mathcal{C}}}(w, v) &:= \begin{cases} 1 & \text{if } w = v, \\ \left(\sum_{i=1}^n a_i \cdot t_{\hat{\mathcal{C}}}(w_i, w) \right)^* \cdot \left(\sum_{i=1}^m b_i \cdot t_{\hat{\mathcal{C}}}(u_i, v) \right) & \text{if } w \leftarrow v, \end{cases} \\
 s_{\hat{\mathcal{C}}}(w) &:= \left(\sum_{i=1}^n a_i \cdot t_{\hat{\mathcal{C}}}(w_i, w) \right)^* \cdot \left(\tau_{\mathcal{C}}(w) + \sum_{i=1}^m b_i \cdot s_{\hat{\mathcal{C}}}(u_i) \right),
 \end{aligned}$$

$$\text{given: } T_{\hat{\mathcal{C}}}(w) = \{ w \xrightarrow{a_i} [u_i] w_i \mid l_i \in \mathbb{N}^+, i \in \{1, \dots, n\} \} \cup \{ w \xrightarrow{b_i} [b_o] u_i \mid i \in \{1, \dots, m\} \},$$

$$\text{induction for } t_{\hat{\mathcal{C}}} \text{ on: } \langle w_1, v_1 \rangle <_{\text{lex}} \langle w_2, v_2 \rangle : \iff v_1 \leftarrow^+ v_2 \vee (v_1 = v_2 \wedge w_1 \leftarrow_{b_o}^+ w_2),$$

$$\text{induction for } s_{\hat{\mathcal{C}}} \text{ on the strict partial order } \leftarrow_{b_o}^+ \text{ (see Lem. 3.1),}$$

where $<_{\text{lex}}$ is a well-founded strict partial order due to Lem. 3.1. The choice of the list representations of action-target sets of $\hat{\mathcal{C}}$ changes these definition only up to provability in ACI .

► **Example 5.2.** We consider the 1-chart \mathcal{C} , and the LLEE-witness $\hat{\mathcal{C}}$ of \mathcal{C} , in the LLEE-witnessed coinductive proof $\mathcal{CP} = \langle \mathcal{C}, L \rangle$ of $(a^* \cdot b^*)^* = (a + b)^*$ in Ex. 4.2. We detail in Fig. 2 the process of computing the principal value $s_{\hat{\mathcal{C}}}(v_s)$ of the extraction function $s_{\hat{\mathcal{C}}}$ of $\hat{\mathcal{C}}$. The statement of Lem. 5.4 below will guarantee that $s_{\hat{\mathcal{C}}}$ is a Mil^- -provable solution of \mathcal{C} .

► **Lemma 5.3.** Let \mathcal{C} be a weakly guarded LLEE-1-chart with guarded LLEE-witness $\hat{\mathcal{C}}$. Then $s_{\hat{\mathcal{C}}}(w) =_{\text{Mil}^-} t_{\hat{\mathcal{C}}}(w, v) \cdot s_{\hat{\mathcal{C}}}(v)$ holds for all vertices $w, v \in V(\mathcal{C})$ such that $w \leftarrow^= v$.

► **Lemma 5.4** (extracted function is provable solution). *Let $\underline{\mathcal{C}}$ be a w.g. LLEE-1-chart with guarded LLEE-witness $\hat{\underline{\mathcal{C}}}$. Then the extraction function $s_{\hat{\underline{\mathcal{C}}}}$ of $\hat{\underline{\mathcal{C}}}$ is a Mil^- -provable solution of $\underline{\mathcal{C}}$.*

► **Lemma 5.5.** *Let $\underline{\mathcal{C}}$ be a 1-chart $\underline{\mathcal{C}}$ with guarded LLEE-witness $\hat{\underline{\mathcal{C}}}$. Let \mathcal{S} be an \mathcal{EL} -based proof system over $\text{StExp}(A)$ such that $\text{ACI} \subseteq \mathcal{S} \lesssim \text{Mil}$.*

Let $s : V(\underline{\mathcal{C}}) \rightarrow \text{StExp}(A)$ be an \mathcal{S} -provable solution of $\underline{\mathcal{C}}$. Then $s(w) =_{\text{Mil}} t_{\hat{\underline{\mathcal{C}}}}(w, v) \cdot s(v)$ holds for all vertices $w, v \in V(\underline{\mathcal{C}})$ with $w \leftarrow^= v$.

For an \mathcal{EL} -based proof system \mathcal{S} over $\text{StExp}(A)$ we say that two star expression functions $s_1, s_2 : V \rightarrow \text{StExp}(A)$ are \mathcal{S} -provably equal if $s_1(v) =_{\mathcal{S}} s_2(v)$ holds for all $v \in V$.

► **Lemma 5.6** (provable equality of solutions of LLEE-1-charts). *Let $\underline{\mathcal{C}}$ be a guarded LLEE-1-chart, and let \mathcal{S} be an \mathcal{EL} -based proof system over $\text{StExp}(A)$ such that $\text{ACI} \subseteq \mathcal{S} \lesssim \text{Mil}$.*

Then any two \mathcal{S} -provable solutions of $\underline{\mathcal{C}}$ are Mil -provably equal.

► **Proposition 5.7.** *For every \mathcal{EL} -based proof system \mathcal{S} over $\text{StExp}(A)$ with $\text{ACI} \subseteq \mathcal{S} \lesssim \text{Mil}$, provability by LLEE-witnessed coinductive proofs over \mathcal{S} implies derivability in Mil :*

$$\left(e_1 \xrightarrow[\mathcal{S}]{\text{LLEE}} e_2 \implies e_1 =_{\text{Mil}} e_2 \right) \quad \text{for all } e_1, e_2 \in \text{StExp}(A). \quad (5.1)$$

Proof. For showing (5.1), let $e, f \in \text{StExp}(A)$ be such that $e \xrightarrow[\mathcal{S}]{\text{LLEE}} f$. Then there is a LLEE-witnessed coinductive proof $\mathcal{CP} = \langle \underline{\mathcal{C}}, L \rangle$ of $e_1 = e_2$ over \mathcal{S} . Then $\underline{\mathcal{C}}$ is a LLEE-1-chart, and there are \mathcal{S} -provable solutions $L_1, L_2 : V(\underline{\mathcal{C}}) \rightarrow \text{StExp}(A)$ of $\underline{\mathcal{C}}$ such that $e_1 \equiv L_1(v_s)$ and $e_2 \equiv L_2(v_s)$. Then L_1 and L_2 are Mil -provably equal by Lem. 5.6. As a consequence we find $e_1 \equiv L_1(v_s) =_{\text{Mil}} L_2(v_s) \equiv e_2$, and hence $e_1 =_{\text{Mil}} e_2$. ◀

► **Example 5.8.** We consider again the LLEE-witnessed coinductive proof $\mathcal{CP} = \langle \underline{\mathcal{C}}, L \rangle$ of $(a^* \cdot b^*)^* = (a + b)^*$ in Ex. 4.2. In Fig. 3 we exhibit the extraction process of derivations in Mil of $L_1(v_s) = s_{\underline{\mathcal{C}}}(v)$ and $L_2(v_s) = s_{\underline{\mathcal{C}}}(v)$ from the LLEE-witness $\hat{\underline{\mathcal{C}}}$ of $\underline{\mathcal{C}}$, which can be combined by \mathcal{EL} rules to obtain a derivation in Mil of $(a^* \cdot b^*)^* \equiv L_1(v_s) = L_2(v_s) \equiv (a + b)^*$.

► **Theorem 5.9.** $\text{cMil} \lesssim \text{Mil}$. *Moreover, every derivation in cMil with conclusion $e = f$ can be transformed effectively into a derivation in Mil that has the same conclusion.*

Proof. It suffices to show the transformation statement. This can be established by a straightforward induction on the depth of derivations in cMil , in which the only non-trivial case is the elimination of LCoProof_n instances. For every instance of LCoProof_n , see Def. 4.1, the induction hypothesis guarantees that the first n premises $g_1 = h_1, \dots, g_n = h_n$ are derivable in Mil . Then the $(n + 1)$ -th premise $\mathcal{LCP}_{\text{Mil}^- + \Gamma}(e = f)$ for $\Gamma := \{g_i = h_i \mid i \in \{1, \dots, n\}\}$ is also a LLEE-witnessed coinductive proof of $e = f$ over Mil . Therefore we can apply Prop. 5.7 in order to obtain a derivation of $e = f$ in Mil , the conclusion of the LCoProof_n instance. ◀

6 From Milner's system to LLEE-witnessed coinductive proofs

In this section we develop a proof-theoretic interpretation of Mil in cMil_1 , and hence in cMil . The crucial step hereby is to show that every instance ι of the fixed-point rule RSP^* of Mil can be mimicked by a LLEE-witnessed coinductive proof over Mil^- in which also the premise of ι may be used. Specifically, an RSP^* -instance with premise $e = f \cdot e + g$ and conclusion $e = f^* \cdot g$ can be translated into a coinductive proof of $e = f^* \cdot g$ over $\text{Mil}^- + \{e = f \cdot e + g\}$ with underlying 1-chart $\underline{\mathcal{C}}(f^* \cdot g)$ and LLEE-witness $\hat{\underline{\mathcal{C}}}(f^* \cdot g)$. While we have illustrated this transformation already in Fig. 1 in the Introduction, we detail it also for a larger example.

$\mathcal{C}, \hat{\mathcal{C}}$

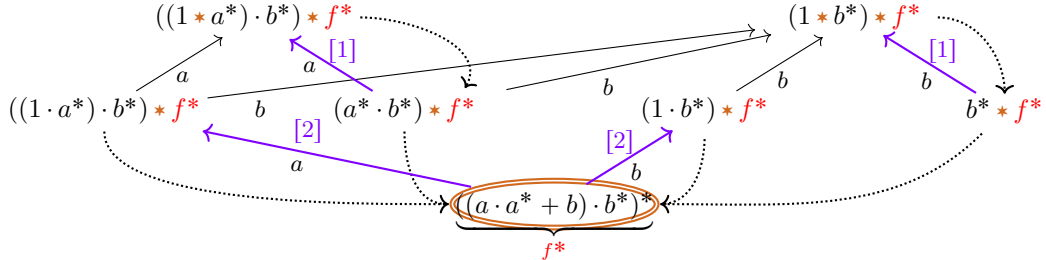
$$\begin{aligned}
 L_i(v_{21}) &= \stackrel{(\text{sol})}{\text{Mil}^-} 1 \cdot L_i(v_2) =_{\text{Mil}^-} L_i(v_2) \\
 & \quad (=_{\text{Mil}^-}^{\text{(sol)}} \text{ means use of 'is Mil}^- \text{-provable solution}') \\
 L_i(v_2) &= \stackrel{(\text{sol})}{\text{Mil}^-} b \cdot L_i(v_{21}) + 1 \cdot L_i(v_s) =_{\text{Mil}^-} b \cdot L_i(v_2) + L_i(v_s) \\
 & \quad \Downarrow \text{applying RSP}^* \\
 L_i(v_2) &=_{\text{Mil}} b^* \cdot L_i(v_s) \\
 L_i(v_{11}) &= \stackrel{(\text{sol})}{\text{Mil}^-} 1 \cdot L_i(v_1) =_{\text{Mil}^-} L_i(v_1) \\
 L_i(v_1) &=_{\text{Mil}^-} a \cdot L_i(v_{11}) + b \cdot L_i(v_{21}) + 1 \cdot L_i(v_s) \\
 &=_{\text{Mil}} a \cdot L_i(v_1) + (b \cdot b^* + 1) \cdot L_i(v_s) \\
 &=_{\text{Mil}^-} a \cdot L_i(v_1) + b^* \cdot L_i(v_s) \\
 & \quad \Downarrow \text{applying RSP}^* \\
 L_i(v_1) &=_{\text{Mil}} a^* \cdot (b^* \cdot L_i(v_s)) =_{\text{Mil}^-} (a^* \cdot b^*) \cdot L_i(v_s) \\
 \\
 L_i(v_s) &= \stackrel{(\text{sol})}{\text{Mil}^-} 1 + a \cdot L_i(v_{11}) + b \cdot L_i(v_{21}) =_{\text{Mil}^-} 1 + a \cdot L_i(v_1) + b \cdot L_i(v_2) \\
 &=_{\text{Mil}} (a \cdot (a^* \cdot b^*) + b \cdot b^*) \cdot L_i(v_s) + 1 \\
 & \quad \Downarrow \text{applying RSP}^* \\
 L_i(v_s) &=_{\text{Mil}} (a \cdot (a^* \cdot b^*) + b \cdot b^*)^* \cdot 1 =_{\text{Mil}^-} (a \cdot (a^* \cdot b^*) + b \cdot b^*)^* =_{\text{Mil}^-} s_{\hat{\mathcal{C}}}(v_s)
 \end{aligned}$$

■ **Figure 3** Use of the LLEE-witness $\hat{\mathcal{C}}$ underlying the coinductive proof $\langle \mathcal{C}, L \rangle$ in Ex. 4.2 for showing that the principal value $L_i(v_s)$ of the Mil^- -provable solution L_i for $i \in \{1, 2\}$ is Mil -provably equal to the principal value $s_{\hat{\mathcal{C}}}(v_s)$ of the solution $s_{\hat{\mathcal{C}}}$ extracted from $\hat{\mathcal{C}}$ (see Fig. 2).

► **Example 6.1.** We consider an instance of RSP^* that corresponds, up to an application of $\text{r-distr}(+, \cdot)$, to the instance of RSP^* at the bottom in Fig. 3:

$$\frac{\overbrace{(a+b)^*}^e = \overbrace{((a \cdot a^* + b) \cdot b^*)}^f \cdot \overbrace{(a+b)^*}^e + \overbrace{1}^g}{\overbrace{(a+b)^*}^e = \overbrace{((a \cdot a^* + b) \cdot b^*)^*}^{f^*} \cdot \overbrace{1}^g} \text{RSP}^* \quad (\text{where } f \downarrow) \quad (6.1)$$

We want to mimic this instance by one of LCoProof_1 that uses a LLEE-witnessed coinductive proof of $e = f^* \cdot g$ over Mil^- plus the premise of the RSP^* instance. We first obtain the 1-chart interpretation $\mathcal{C}(f^*)$ of f^* according to Def. 3.2 together with its LLEE-witness $\hat{\mathcal{C}}(f^*)$:



Due to Lem. 3.5 the iterated partial 1-derivatives as depicted define a Mil^- -provable solution of $\mathcal{C}(f^*)$ when stacked products $*$ are replaced by products \cdot . From this LLEE-witness that carries a Mil -provable solution we now obtain a LLEE-witnessed coinductive proof of $f \cdot e + g = f^* \cdot g$ under the assumption of $e = f \cdot e + g$, as follows. By replacing parts $(\dots) * f^*$

by $\pi((\dots)) \cdot e$ in the Mil-provable solution of $\underline{\mathcal{C}}(f^*)$, and respectively, by replacing $(\dots) \star f^*$ by $(\pi((\dots)) \cdot f^*) \cdot g$ we obtain the left- and the right-hand sides of the formal equations below:

$$\begin{array}{c}
 ((1 \cdot a^*) \cdot b^*) \cdot e = (((1 \cdot a^*) \cdot b^*) \cdot f^*) \cdot g \qquad (1 \cdot b^*) \cdot e = ((1 \cdot b^*) \cdot f^*) \cdot g \\
 \begin{array}{ccc}
 \nearrow a & \nwarrow a & \nearrow b \\
 & [1] & \\
 (a^* \cdot b^*) \cdot e = ((a^* \cdot b^*) \cdot f^*) \cdot g & & b^* \cdot e = (b^* \cdot f^*) \cdot g
 \end{array} \\
 ((1 \cdot a^*) \cdot b^*) \cdot e = (((1 \cdot a^*) \cdot b^*) \cdot f^*) \cdot g \qquad (1 \cdot b^*) \cdot e = ((1 \cdot b^*) \cdot f^*) \cdot g \\
 \begin{array}{ccc}
 \nwarrow a & \nearrow b & \\
 & [2] & \\
 \underbrace{((a \cdot a^* + b) \cdot b^*) \cdot (a + b)^* + 1}_{f \quad e \quad g} = \underbrace{(((a \cdot a^* + b) \cdot b^*)^* \cdot 1)}_{f^* \quad g} \\
 = e \text{ (by rule assumption)}
 \end{array}
 \end{array}$$

This is a LLEE-witnessed coinductive proof \mathcal{LCP} of $f \cdot e + g = f^* \cdot g$ over $\text{Mil}^- + \{e = f \cdot e + g\}$: The right-hand sides form a Mil-provable solution of $\mathcal{C}(f^* \cdot g)$ due to Lemma 3.5 (note that $\mathcal{C}(f^* \cdot g)$ is isomorphic to $\mathcal{C}(f^*)$ due to $g \equiv 1$). The left-hand sides also form a solution of $\mathcal{C}(f^* \cdot g)$ (see Lem. 6.2 below), noting that for the 1-transitions back to the conclusion the assumption $e = f \cdot e + g$ must be used in addition to Mil^- . By using this assumption again, the result \mathcal{LCP}' of replacing $f \cdot e + g$ in the conclusion of \mathcal{LCP} by e is also a LLEE-witnessed coinductive proof over $\text{Mil}^- + \{e = f \cdot e + g\}$. Consequently:

$$\frac{e = f \cdot e + g \quad \mathcal{LCP}_{\text{Mil}^- + \{e = f \cdot e + g\}}(e = f^* \cdot g)}{e = f^* \cdot g} \text{LCoProof}_1$$

is a rule instance of cMil and CLC by which we have mimicked the RSP^* instance in (6.1).

► **Lemma 6.2.** *Let $e, f, g \in \text{StExp}(A)$ with $f \downarrow$, and let $\Gamma := \{e = f \cdot e + g\}$. Then e is the principal value of a $(\text{Mil}^- + \Gamma)$ -provable solution of the 1-chart interpretation $\underline{\mathcal{C}}(f^* \cdot g)$ of $f^* \cdot g$.*

Proof. First, it can be verified that the vertices of $\underline{\mathcal{C}}(f^* \cdot g)$ are of either of three forms:

$$V(\underline{\mathcal{C}}(f^* \cdot g)) = \{f^* \cdot g\} \cup \{(F \star f^*) \cdot g \mid F \in \underline{\partial}^+(f)\} \cup \{G \mid G \in \underline{\partial}^+(g)\},$$

where $\underline{\partial}^+(f)$ means the set of iterated 1-derivatives of f according to the TSS in Def. 3.2. This facilitates to define a star expression function $s : V(\underline{\mathcal{C}}(f^* \cdot g)) \rightarrow \text{StExp}(A)$ on $\underline{\mathcal{C}}(f^* \cdot g)$ by:

$$s(f^* \cdot g) := e, \quad s((F \star f^*) \cdot g) := \pi(F) \cdot e, \quad s(G) := \pi(G),$$

for all $F \in \underline{\partial}^+(f)$ and $G \in \underline{\partial}^+(g)$. We show that s is a $(\text{Mil}^- + \Gamma)$ -provable solution of $\underline{\mathcal{C}}(f^* \cdot g)$.

For this, we have to show that s is $(\text{Mil}^- + \Gamma)$ -provable at each of the three kinds of vertices of $\underline{\mathcal{C}}(f^* \cdot g)$, namely at $f^* \cdot g$, at $(F \star f^*) \cdot g$ with $F \in \underline{\partial}^+(f)$, and at G with $G \in \underline{\partial}^+(g)$. Here we only consider $f^* \cdot g$, because it is the single case in which the assumption in Γ has to be used, and the two other forms can be argued similarly (please see in the appendix). By $\underline{A\partial}(H) := \{\langle a, H' \rangle \mid H \xrightarrow{a} H'\}$ we denote the set of ‘‘action 1-derivatives’’ of a stacked star expression H . In the following argument we avoid list representations of transitions

16:16 A Coinductive Version of Milner's Proof System

(as in Def. 2.7) in favor of arguing with sums over sets of action derivatives that represent ACI-equivalence classes of star expressions. This shorthand is possible due to $\text{ACI} \subseteq \text{Mil}^-$.

$$\begin{aligned}
s(f^* \cdot g) &\equiv e && \text{(by the definition of } s) \\
&=_{\text{Mil}^- + \Gamma} f \cdot e + g && \text{(since } \Gamma = \{e = f \cdot e + g\}) \\
&=_{\text{Mil}^-} \left(\tau_{\underline{\mathcal{C}}(f)}(f) + \sum_{\langle \underline{a}, F \rangle \in \underline{\mathcal{A}\hat{\mathcal{C}}}(f)} \underline{a} \cdot \pi(F) \right) \cdot e + \left(\tau_{\underline{\mathcal{C}}(g)}(g) + \sum_{\langle \underline{a}, G \rangle \in \underline{\mathcal{A}\hat{\mathcal{C}}}(g)} \underline{a} \cdot \pi(G) \right) && \text{(by using Lem. 3.4)} \\
&=_{\text{Mil}^-} \left(\sum_{\langle \underline{a}, F \rangle \in \underline{\mathcal{A}\hat{\mathcal{C}}}(f)} \underline{a} \cdot (\pi(F) \cdot e) \right) + \left(\tau_{\underline{\mathcal{C}}(f^* \cdot g)}(f^* \cdot g) + \sum_{\langle \underline{a}, G \rangle \in \underline{\mathcal{A}\hat{\mathcal{C}}}(g)} \underline{a} \cdot \pi(G) \right) && \text{(by (assoc(\cdot)), (r-distr(+, \cdot)), (deadlock))} \\
&\quad \text{(using } \tau_{\underline{\mathcal{C}}(f)}(f) \equiv 0 \text{ due to } f \downarrow, \text{ and } \tau_{\underline{\mathcal{C}}(f^* \cdot g)}(f^* \cdot g) \equiv \tau_{\underline{\mathcal{C}}(g)}(g)) \\
&=_{\text{ACI}} \tau_{\underline{\mathcal{C}}(f^* \cdot g)}(f^* \cdot g) + \left(\sum_{\langle \underline{a}, F \rangle \in \underline{\mathcal{A}\hat{\mathcal{C}}}(f)} \underline{a} \cdot (s((F * f^*) \cdot g)) \right) + \sum_{\langle \underline{a}, G \rangle \in \underline{\mathcal{A}\hat{\mathcal{C}}}(g)} \underline{a} \cdot s(G) \\
&\quad \text{(by definition of } s, \text{ axioms (comm(+)))} \\
&=_{\text{ACI}} \tau_{\underline{\mathcal{C}}(f^* \cdot g)}(f^* \cdot g) + \sum_{\langle \underline{a}, E' \rangle \in \underline{\mathcal{A}\hat{\mathcal{C}}}(f^* \cdot g)} \underline{a} \cdot s(E') \\
&\quad \text{(since } \underline{\mathcal{A}\hat{\mathcal{C}}}(f^* \cdot g) = \{\langle \underline{a}, (F * f^*) \cdot g \rangle \mid \langle \underline{a}, F \rangle \in \underline{\mathcal{A}\hat{\mathcal{C}}}(f)\} \cup \underline{\mathcal{A}\hat{\mathcal{C}}}(g) \\
&\quad \text{by inspection of the TSS in Def. 3.2).}
\end{aligned}$$

Due to $\text{ACI} \subseteq \text{Mil}^- \subseteq \text{Mil}^- + \Gamma$, the above chain of equalities is provable in $\text{Mil}^- + \Gamma$. Therefore it demonstrates, for any given list representation of $\tau_{\underline{\mathcal{C}}(f^* \cdot g)}(f^* \cdot g)$ according to the correctness condition in Def. 2.7, that s is a $(\text{Mil}^- + \Gamma)$ -provable solution of $\underline{\mathcal{C}}(f^* \cdot g)$ at $f^* \cdot g$. ◀

► **Lemma 6.3.** *Let $e, f, g \in \text{StExp}(A)$ with $f \downarrow$, and let $\Gamma := \{e = f \cdot e + g\}$. Then it holds that $e \stackrel{\text{LLEE}}{=}_{(\text{Mil}^- + \Gamma)} f^* \cdot g$.*

Proof. By Lem. 6.2 there is a $\text{Mil}^- + \Gamma$ -provable solution s_1 of $\underline{\mathcal{C}}(f^* \cdot g)$ with $s_1(f^* \cdot g) \equiv e$. By Lem. 3.5 there is a Mil^- -provable solution s_2 of $\underline{\mathcal{C}}(f^* \cdot g)$ with $s_2(f^* \cdot g) \equiv f^* \cdot g$. Then $\langle \underline{\mathcal{C}}(f^* \cdot g), L \rangle$ with $L(v) := s_1(v) = s_2(v)$ for all $v \in V(\underline{\mathcal{C}}(f^* \cdot g))$ is a LLEE-witnessed coinductive proof of $e = f^* \cdot g$ over $\text{Mil}^- + \Gamma$, as $\underline{\mathcal{C}}(f^* \cdot g)$ has LLEE-witness $\hat{\underline{\mathcal{C}}}(f^* \cdot g)$ by Thm. 3.3. ◀

► **Theorem 6.4.** $\text{Mil} \lesssim \text{cMil}_1$. *What is more, every derivation in Mil with conclusion $e = f$ can be transformed effectively into a derivation with conclusion $e = f$ in cMil_1 .*

Proof. Every derivation \mathcal{D} in Mil can be transformed into a derivation \mathcal{D}' in cMil_1 with the same conclusion as \mathcal{D} by replacing every instance of RSP^* in \mathcal{D} by a mimicking derivation in cMil_1 as in the following step, where $f \downarrow$ holds as the side-condition of the instance of RSP^* :

$$\frac{e = f \cdot e + g}{e = f^* \cdot g} \text{RSP}^* \quad \Longrightarrow \quad \frac{e = f \cdot e + g \quad \mathcal{LCP}_{\text{Mil}^- + \Gamma}(e = f^* \cdot g)}{e = f^* \cdot g} \text{LCoProof}_1$$

and where $\mathcal{LCP}_{\text{Mil}^- + \Gamma}(e = f^* \cdot g)$ is, for $\Gamma := \{e = f \cdot e + g\}$, a LLEE-witnessed coinductive proof over $\text{Mil}^- + \Gamma$ of $e = f^* \cdot g$ that is guaranteed by Lem. 6.3. ◀

► **Theorem 6.5.** $\text{Mil} \sim \text{cMil}_1 \sim \text{cMil} \sim \text{CLC}$, *i.e. these proof systems are theorem-equivalent.*

Proof. Due to $\text{Mil} \lesssim \text{cMil}_1 \lesssim \text{cMil} (\sim \text{CLC}) \lesssim \text{Mil}$ by Thm. 6.4, Lem. 4.7, and Thm. 5.9. ◀

7 Conclusion

In order to increase the options for a completeness proof of Milner’s system Mil for the process semantics of regular expressions under bisimilarity, we set out to formulate proof systems of equal strength half-way in between Mil and bisimulations between star expressions. Specifically we aimed at characterizing the derivational power that the fixed-point rule RSP^* in Mil adds to its purely equational part Mil^- . We based our development on a crucial step from the completeness proof [11] for a tailored restriction of Mil to “1-free” star expressions: guarded linear specifications with the (layered) loop existence and elimination property (L)LEE [7, 11] are uniquely solvable in Mil . We have obtained the following concepts and results:

- As LLEE-witnessed coinductive proof we defined any weakly guarded LLEE-1-chart \mathcal{C} whose vertices are labeled by equations between the values of two provable solutions of \mathcal{C} .
- Based on such proofs, we defined a coinductive version $cMil$ of Milner’s system Mil , and as its “kernel” a system CLC for merely combining LLEE-witnessed coinductive proofs.
- Via proof transformations we showed that $cMil$ and CLC are theorem-equivalent to Mil .
- Based on coinductive proofs without LLEE-witnesses, we formulated systems \overline{cMil} and CC that can be shown to be complete, as can a variant \overline{Mil}' of Mil with the strong rule USP .

Since the proof systems $cMil$ and CLC are tied to process graphs via the circular deductions they permit, and as they are theorem-equivalent with Mil , they may become natural beachheads for a completeness proof of Milner’s system. Indeed, they can be linked to the completeness proof in [11]: it namely guarantees that valid equations between “1-free” star expressions can always be mimicked by derivations in CLC of depth 2. This suggests the following question:

- ▷ Can derivations in CLC (in $cMil$) always be simplified to some (kind of) normal form that is of bounded depth (resp., of bounded nesting depth of LLEE-witn. coinductive proofs)?

Investigating workable concepts of “normal form” for derivations in CLC or in $cMil$, by using simplification steps of process graphs with LEE and 1-transitions under 1-bisimilarity as developed for the completeness proof for “1-free” star expressions in [11], is our next goal.

References

- 1 Roberto M. Amadio and Luca Cardelli. Subtyping Recursive Types. *ACM Trans. Program. Lang. Syst.*, 15(4):575–631, September 1993. doi:10.1145/155183.155231.
- 2 Valentin Antimirov. Partial Derivatives of Regular Expressions and Finite Automaton Constructions. *Theoretical Computer Science*, 155(2):291–319, 1996. doi:10.1016/0304-3975(95)00182-4.
- 3 Michael Brandt and Fritz Henglein. Coinductive Axiomatization of Recursive Type Equality and Subtyping. *Fundamenta Informaticae*, 33(4):309–338, December 1998. doi:10.1007/3-540-62688-3_29.
- 4 Clemens Grabmayer. *Relating Proof Systems for Recursive Types*. PhD thesis, Vrije Universiteit Amsterdam, March 2005. www.phil.uu.nl/~clemens/linkedfiles/proefschrift.pdf.
- 5 Clemens Grabmayer. Using Proofs by Coinduction to Find “Traditional” Proofs. In José Luiz Fiadeiro, Neal Harman, Markus Roggenbach, and Jan Rutten, editors, *Proceedings of CALCO 2005*, volume 3629 of *LNCS*, pages 175–193. Springer, 2005.
- 6 Clemens Grabmayer. A Coinductive Axiomatisation of Regular Expressions under Bisimulation. Technical report, University of Nottingham, 2006. Short Contribution to CMCS 2006, March 25-27, 2006, Vienna Institute of Technology, Austria.
- 7 Clemens Grabmayer. Modeling Terms by Graphs with Structure Constraints (Two Illustrations). In *Proc. TERMGRAPH@FSCD’18*, volume 288, pages 1–13, <http://www.eptcs.org/>, 2019. EPTCS. doi:10.4204/EPTCS.288.1.

- 8 Clemens Grabmayer. Structure-Constrained Process Graphs for the Process Semantics of Regular Expressions. Technical report, [arxiv.org](https://arxiv.org/abs/2012.10869), December 2020. [arXiv:2012.10869](https://arxiv.org/abs/2012.10869).
- 9 Clemens Grabmayer. A Coinductive Version of Milner's Proof System for Regular Expressions Modulo Bisimilarity. Technical report, [arxiv.org](https://arxiv.org/abs/2108.13104), August 2021. Extended version of this paper. [arXiv:2108.13104](https://arxiv.org/abs/2108.13104).
- 10 Clemens Grabmayer. Structure-Constrained Process Graphs for the Process Semantics of Regular Expressions. In Patrick Bahr, editor, Proceedings 11th International Workshop on *Computing with Terms and Graphs*, Online, 5th July 2020, volume 334 of *Electronic Proceedings in Theoretical Computer Science*, pages 29–45. Open Publishing Association, 2021. [doi:10.4204/EPTCS.334.3](https://doi.org/10.4204/EPTCS.334.3).
- 11 Clemens Grabmayer and Wan Fokink. A Complete Proof System for 1-Free Regular Expressions Modulo Bisimilarity. In *Proceedings of LICS 2020*, New York, NY, 2020. ACM. Extended report see [12].
- 12 Clemens Grabmayer and Wan Fokink. A Complete Proof System for 1-Free Regular Expressions Modulo Bisimilarity. Technical report, [arxiv.org](https://arxiv.org/abs/2004.12740), April 2020. [arXiv:2004.12740](https://arxiv.org/abs/2004.12740).
- 13 Robin Milner. A Complete Inference System for a Class of Regular Behaviours. *Journal of Computer and System Sciences*, 28(3):439–466, 1984.
- 14 Arto Salomaa. Two Complete Axiom Systems for the Algebra of Regular Events. *Journal of the ACM*, 13(1):158–169, 1966. [doi:10.1145/321312.321326](https://doi.org/10.1145/321312.321326).

A Appendix: Supplements

This appendix has two parts: In Section A.1, we justify the coinductive proofs we exhibited in Section 1. In Section A.2, we provide remaining details of a lemma that is crucial for the construction of the transformation from the coinductive system \mathbf{cMil} to Milner's system \mathbf{Mil} .

A.1 Justification of coinductive proofs in Section 1

Here we provide justifications for the coinductive proof on page 2, in Ex. A.1 below, and for the coinductive proof in Fig. 1, in Ex. A.2 below.

► **Example A.1** (LLEE-witnessed coinductive proof on page 2). In Section 1 on page 2 we displayed, for the statement $g^* \cdot 0 \equiv (a + b)^* \cdot 0 \stackrel{\text{LLEE}}{\equiv}_{\mathbf{Mil}^-} (a \cdot (a + b) + b)^* \cdot 0 \equiv h^* \cdot 0$ the coinductive proof $\mathcal{CP} = \langle \underline{\mathcal{C}}(h^* \cdot 0), L \rangle$ over \mathbf{Mil}^- with underlying LLEE-witness $\hat{\mathcal{C}}(h^* \cdot 0)$, where $\underline{\mathcal{C}}(h^* \cdot 0)$ and $\hat{\mathcal{C}}(h^* \cdot 0)$ are defined according to Def. 3.2 and the equation-labeling function L on $\underline{\mathcal{C}}(h^* \cdot 0)$ is defined by the illustration that we repeat here:

$$\begin{array}{c}
 (1 \cdot g^*) \cdot 0 = ((1 \cdot (a + b)) \cdot h^*) \cdot 0 \xrightarrow{a, b} (1 \cdot g^*) \cdot 0 = (1 \cdot h^*) \cdot 0 \\
 \begin{array}{ccc}
 \swarrow a \quad [1] & & \searrow b \quad [1] \\
 \underbrace{(a + b)^* \cdot 0}_{g^*} & = & \underbrace{(a \cdot (a + b) + b)^* \cdot 0}_{h^*} \\
 & & \leftarrow 1
 \end{array}
 \end{array}
 \quad
 \begin{array}{c}
 \bullet \xrightarrow{a, b} \bullet \\
 \swarrow a \quad [1] \quad \searrow b \quad [1] \\
 \hat{\mathcal{C}}(h^* \cdot 0) \\
 \leftarrow 1
 \end{array}$$

The correctness conditions at the start vertex (at the bottom) can be verified as follows:

$$\begin{aligned}
 g^* \cdot 0 &\equiv (a + b)^* \cdot 0 \stackrel{\text{Mil}^-}{=} (1 + (a + b) \cdot (a + b)^*) \cdot 0 \stackrel{\text{Mil}^-}{=} 1 \cdot 0 + ((a + b) \cdot g^*) \cdot 0 \\
 &\stackrel{\text{Mil}^-}{=} 0 + (a \cdot g^* + b \cdot g^*) \cdot 0 \stackrel{\text{Mil}^-}{=} (a \cdot g^* + b \cdot g^*) \cdot 0 \\
 &\stackrel{\text{Mil}^-}{=} (a \cdot g^*) \cdot 0 + (b \cdot g^*) \cdot 0 \stackrel{\text{Mil}^-}{=} a \cdot (g^* \cdot 0) + b \cdot (g^* \cdot 0) \\
 &\stackrel{\text{Mil}^-}{=} a \cdot ((1 \cdot g^*) \cdot 0) + b \cdot ((1 \cdot g^*) \cdot 0), \\
 h^* \cdot 0 &\equiv (a \cdot (a + b) + b)^* \cdot 0 \stackrel{\text{Mil}^-}{=} (1 + (a \cdot (a + b) + b) \cdot (a \cdot (a + b) + b)^*) \cdot 0
 \end{aligned}$$

$$\begin{aligned}
&=_{\text{Mil}^-} 1 \cdot 0 + ((a \cdot (a + b) + b) \cdot h^*) \cdot 0 =_{\text{Mil}^-} 0 + ((a \cdot (a + b)) \cdot h^* + b \cdot h^*) \cdot 0 \\
&=_{\text{Mil}^-} (a \cdot ((a + b) \cdot h^*) + b \cdot h^*) \cdot 0 =_{\text{Mil}^-} ((a \cdot ((a + b) \cdot h^*)) \cdot 0 + (b \cdot h^*) \cdot 0) \\
&=_{\text{Mil}^-} a \cdot ((a + b) \cdot h^*) \cdot 0 + b \cdot (h^* \cdot 0) \\
&=_{\text{Mil}^-} a \cdot ((1 \cdot (a + b)) \cdot h^*) \cdot 0 + b \cdot ((1 \cdot h^*) \cdot 0).
\end{aligned}$$

From the provable equality for $g^* \cdot 0$ the correctness condition for $(1 \cdot g^*) \cdot 0$ at the left upper vertex of $\underline{\mathcal{C}}(h^* \cdot 0)$ can be obtained by additional uses of the axiom $(\text{id}_1(\cdot))$. The correctness condition for $((1 \cdot (a + b)) \cdot h^*) \cdot 0$ at the left upper vertex of $\underline{\mathcal{C}}(h^* \cdot 0)$ can be verified as follows:

$$\begin{aligned}
((1 \cdot (a + b)) \cdot h^*) \cdot 0 &=_{\text{Mil}^-} ((a + b) \cdot h^*) \cdot 0 =_{\text{Mil}^-} (a \cdot h^* + b \cdot h^*) \cdot 0 \\
&=_{\text{Mil}^-} (a \cdot h^*) \cdot 0 + (b \cdot h^*) \cdot 0 =_{\text{Mil}^-} a \cdot (h^* \cdot 0) + b \cdot (h^* \cdot 0) \\
&=_{\text{Mil}^-} a \cdot ((1 \cdot h^*) \cdot 0) + b \cdot ((1 \cdot h^*) \cdot 0).
\end{aligned}$$

Finally, the correctness conditions at the right upper vertex of $\underline{\mathcal{C}}(h^* \cdot 0)$ can be obtained by applications of the axiom $(\text{id}_1(\cdot))$ only.

► **Example A.2** (LLEE-witnessed coinductive proof in Fig. 1). We provided a first illustration for translating an instance of the fixed-point rule into a coinductive proof in Figure 1 on page 3. Specifically, we mimicked the instance ι (see below) of the fixed-point rule RSP^* in Milner's system $\text{Mil} = \text{Mil}^- + \text{RSP}^*$ by a coinductive proof (see also below) over $\text{Mil}^- + \{\text{premise of } \iota\}$ with LLEE-witness $\hat{\mathcal{C}}(f^* \cdot 0)$:

$$\begin{array}{c}
\frac{\overbrace{(a+b)^* \cdot 0}^{e_0^*} = \overbrace{(a \cdot (a+b) + b)}^f \cdot \overbrace{(a+b)^* \cdot 0}^{e_0^*} + 0}{(a+b)^* \cdot 0 = (a \cdot (a+b) + b)^* \cdot 0} \quad \iota, \text{RSP}^* \frac{e_0^* \cdot 0 = f \cdot (e_0^* \cdot 0) + 0}{e_0^* \cdot 0 = f^* \cdot 0} \\
\\
(1 \cdot (a+b)) \cdot (e_0^* \cdot 0) = ((1 \cdot (a+b)) \cdot f^*) \cdot 0 \xrightarrow{a, b} 1 \cdot (e_0^* \cdot 0) = (1 \cdot f^*) \cdot 0 \\
\hat{\mathcal{C}}(f^* \cdot 0) \xleftarrow{a} \underbrace{e_0^* \cdot 0}_f = \underbrace{(a \cdot (a+b) + b)^* \cdot 0}_{f^*} \xrightarrow{b} 1 \cdot (e_0^* \cdot 0) \xleftarrow{1} 1 \\
\text{(by the premise of } \iota) \quad (a \cdot (a+b) + b) \cdot (e_0^* \cdot 0) + 0 \equiv f \cdot (e_0^* \cdot 0) + 0 =
\end{array}$$

The correctness conditions for the right-hand sides of this proof tree to be a LLEE-witnessed coinductive proof $\text{Mil}^- + \{\text{premise of } \iota\}$ are the same as those that we have verified for the right-hand sides of the coinductive proof over Mil^- with the same LLEE-witness in Ex. A.1. Note that the premise of ι is not used for the correctness conditions of the right-hand sides. The correctness condition for the left-hand side $e_0^* \cdot 0$ at the bottom vertex of $\underline{\mathcal{C}}(f^* \cdot 0)$ can be verified as follows, now making use of the premise of the considered instance ι of RSP^* :

$$\begin{aligned}
e_0^* \cdot 0 &=_{\{\text{premise of } \iota\}} f \cdot (e_0^* \cdot 0) + 0 =_{\text{Mil}^-} (a \cdot (a + b) + b) \cdot (e_0^* \cdot 0) \\
&=_{\text{Mil}^-} (a \cdot (a + b)) \cdot (e_0^* \cdot 0) + b \cdot (e_0^* \cdot 0) \\
&=_{\text{Mil}^-} a \cdot ((a + b) \cdot (e_0^* \cdot 0)) + b \cdot (1 \cdot (e_0^* \cdot 0)) \\
&=_{\text{Mil}^-} a \cdot ((1 \cdot (a + b)) \cdot (e_0^* \cdot 0)) + b \cdot (1 \cdot (e_0^* \cdot 0))
\end{aligned}$$

Together this yields the provable equation:

$$e_0^* \cdot 0 =_{\text{Mil}^- + \{\text{premise of } \iota\}} a \cdot ((1 \cdot (a + b)) \cdot (e_0^* \cdot 0)) + b \cdot (1 \cdot (e_0^* \cdot 0)),$$

which demonstrates the correctness condition for the left-hand side $e_0^* \cdot 0$ at the bottom vertex of $\underline{\mathcal{C}}(f^* \cdot 0)$. The correctness condition for the left-hand side $a \cdot ((1 \cdot (a + b)))$ at the top left vertex of $\underline{\mathcal{C}}(f^* \cdot 0)$ can be verified without using the premise of ι as follows:

$$\begin{aligned} ((1 \cdot (a + b)) \cdot (e_0^* \cdot 0)) &=_{\text{Mil}^-} ((a + b) \cdot (e_0^* \cdot 0)) =_{\text{Mil}^-} a \cdot (e_0^* \cdot 0) + b \cdot (e_0^* \cdot 0) \\ &=_{\text{Mil}^-} a \cdot (1 \cdot (e_0^* \cdot 0)) + b \cdot (1 \cdot (e_0^* \cdot 0)). \end{aligned}$$

Finally, the correctness condition of the left-hand side $1 \cdot (e_0^* \cdot 0)$ at the right upper vertex of $\underline{\mathcal{C}}(f^* \cdot 0)$ can be obtained by an application of the axiom $(\text{id}_1(\cdot))$ only.

A.2 Completing the proof of Lemma 6.2

Here we provide those remaining details for the proof of Lem. 6.2 that we have postponed from within the proof environment on page 15. This lemma is crucial for the construction of the proof transformation from the coinductive system cMil to Milner's system Mil (see Thm. 6.4), which proceeds by mimicking arbitrary instances ι of the fixed-point rule RSP^* by coinductive proofs over the equational part Mil^- of Mil plus the premise of ι (see Lem. 6.3). Indeed, Lem. 6.2 provides, for every generic instance ι of RSP^* as in Def. 2.4, a provable solution for the 1-chart interpretation $\underline{\mathcal{C}}(f^* \cdot g)$ of $f^* \cdot g$ that can provide (see Lem. 6.3) the left-hand sides of the equations in a coinductive proof that mimics ι .

► **Lemma** (= Lem. 6.2). *Let $e, f, g \in \text{StExp}(A)$ with $f \downarrow$, and let $\Gamma := \{e = f \cdot e + g\}$. Then the star expression e is the principal value of a $(\text{Mil}^- + \Gamma)$ -provable solution of the 1-chart interpretation $\underline{\mathcal{C}}(f^* \cdot g)$ of $f^* \cdot g$.*

Before we extend the proof of this lemma from page 15 by treating the cases that we have not yet treated, we gather and outline the proofs of auxiliary statements that are used in the proof of Lem. 6.2. The first lemma concerns the set of *action 1-derivatives* of a star expression, or stacked star expression, over set A of actions, defined by $\underline{A\partial}(E) := \{\langle a, E' \rangle \mid E \xrightarrow{a} E'\}$, where the transitions are defined by the TSS in Def. 3.2.

► **Lemma A.3.** *The action 1-derivatives $\underline{A\partial}(E)$ of a stacked star expression E over actions in A satisfy the following recursive equations, for all $a \in A$, $e, e_1, e_2 \in \text{StExp}(A)$, and stacked star expressions E_1 over actions in A :*

$$\begin{aligned} \underline{A\partial}(0) &:= \underline{A\partial}(1) := \emptyset, \\ \underline{A\partial}(a) &:= \{\langle a, 1 \rangle\}, \\ \underline{A\partial}(e_1 + e_2) &:= \underline{A\partial}(e_1) \cup \underline{A\partial}(e_2), \\ \underline{A\partial}(E_1 \cdot e_2) &:= \begin{cases} \{\langle a, E'_1 \cdot e_2 \rangle \mid \langle a, E'_1 \rangle \in \underline{A\partial}(E_1)\} & \text{if } E_1 \downarrow, \\ \{\langle a, E'_1 \cdot e_2 \rangle \mid \langle a, E'_1 \rangle \in \underline{A\partial}(E_1)\} \cup \underline{A\partial}(E_2) & \text{if } E_1 \downarrow, \end{cases} \\ \underline{A\partial}(E_1 * e_2^*) &:= \begin{cases} \{\langle a, E'_1 \cdot e_2^* \rangle \mid \langle a, E'_1 \rangle \in \underline{A\partial}(E_1)\} & \text{if } E_1 \downarrow, \\ \{\langle a, E'_1 \cdot e_2^* \rangle \mid \langle a, E'_1 \rangle \in \underline{A\partial}(E_1)\} \cup \{\langle 1, e_2^* \rangle\} & \text{if } E_1 \downarrow, \end{cases} \\ \underline{A\partial}(e^*) &:= \{\langle a, E' * e^* \rangle \mid \langle a, E' \rangle \in \underline{A\partial}(e)\}. \end{aligned} \tag{A.1}$$

Proof. By case-wise inspection of the definition of the TSS in Def. 3.2. ◀

For the proof of Lem. 3.4 we will need the following auxiliary statement.

► **Lemma A.4.** *If $e \downarrow$ for a star expression $e \in \text{StExp}(A)$, then there is a star expression $f \in \text{StExp}(A)$ with $f \downarrow$, $e =_{\text{Mil}^-} 1 + f$, $|f|_* = |e|_*$, and $((\text{id} \times \pi) \circ \underline{A\partial})(f) = ((\text{id} \times \pi) \circ \underline{A\partial})(e)$.*

Proof. By a proof by induction on structure of e , in which all axioms of Mil^- are used. ◀

► **Lemma A.5** (corresponds to Lem. 3.4). $\pi(E) =_{\text{Mil}^-} \tau_{\underline{\mathcal{C}}(E)}(E) + \sum_{\langle \underline{a}, E' \rangle \in \underline{A\hat{\mathcal{C}}}(E)} \underline{a} \cdot \pi(E')$, for all stacked star expressions E over actions in A , (where we permit that the sum expression on the right indicates a star expression only up to ACI (note that $\text{ACI} \subseteq \text{Mil}^-$)).

Proof. The statement of the lemma can be proved by induction on the structure of the stacked star expression E with a subinduction on the syntactical star height $|E|_*$ of E . All cases of stacked star expressions can be dealt with in a straightforward manner, except for those with an outermost iteration where in a subcase the subinduction hypothesis must be used.

Suppose that $E \equiv e^*$, and that $e \downarrow$ holds. Then by Lem. A.4 there exists a star expression f such that $f \downarrow$, $e =_{\text{Mil}^-} 1 + f$, $|f|_* = |e|_*$, and $((\text{id} \times \pi) \circ \underline{A\hat{\mathcal{C}}})(f) = ((\text{id} \times \pi) \circ \underline{A\hat{\mathcal{C}}})(e)$. Then we can argue as follows to prove the desired Mil^- -provable equation for $\pi(E)$, where we apply the subinduction hypothesis for $\pi(f)$, which is possible due to $|f|_* = |e|_* < 1 + |e|_* = |e^*|_* = |E|_*$:

$$\begin{aligned} \pi(E) &\equiv \pi(e^*) \equiv e^* =_{\text{Mil}^-} (1 + f)^* =_{\text{Mil}^-} f^* =_{\text{Mil}^-} 1 + f \cdot f^* \\ &=_{\text{Mil}^-} 1 + f \cdot (1 + f)^* =_{\text{Mil}^-} 1 + f \cdot e^* \equiv 1 + \pi(f) \cdot e^* \\ &=_{\text{Mil}^-} 1 + (\tau_{\underline{\mathcal{C}}(f)}(f) + \sum_{\langle \underline{a}, F' \rangle \in \underline{A\hat{\mathcal{C}}}(f)} \underline{a} \cdot \pi(F')) \cdot e^* \\ &\equiv 1 + (0 + \sum_{\langle \underline{a}, F' \rangle \in \underline{A\hat{\mathcal{C}}}(f)} \underline{a} \cdot \pi(F')) \cdot e^* \\ &=_{\text{Mil}^-} \tau_{\underline{\mathcal{C}}(e^*)}(e^*) + \sum_{\langle \underline{a}, E' \rangle \in \underline{A\hat{\mathcal{C}}}(e)} \underline{a} \cdot (\pi(E') \cdot e^*) \\ &=_{\text{Mil}^-} \tau_{\underline{\mathcal{C}}(e^*)}(e^*) + \sum_{\langle \underline{a}, E' \rangle \in \underline{A\hat{\mathcal{C}}}(e)} \underline{a} \cdot \pi(E' * e^*) \\ &=_{\text{Mil}^-} \tau_{\underline{\mathcal{C}}(E)}(E) + \sum_{\langle \underline{a}, E' \rangle \in \underline{A\hat{\mathcal{C}}}(E)} \underline{a} \cdot \pi(E'), \end{aligned}$$

where in the last step we used the representation of $\underline{A\hat{\mathcal{C}}}(E) = \underline{A\hat{\mathcal{C}}}(e^*)$ according to (A.1).

In the case that $E = e^*$ with $e \downarrow$ we can reason similarly but simpler, because then it is sufficient to use the induction hypothesis for e , which is structurally simpler than e^* . ◀

► **Lemma** (= Lem. 3.5). For every star expression $e \in \text{StExp}(A)$ with 1-chart interpretation $\underline{\mathcal{C}}(e) = \langle V(e), A, 1, e, \rightarrow, \downarrow \rangle$ the star-expression function $s : V(e) \rightarrow \text{StExp}(A)$, $E \mapsto \pi(E)$ is a Mil^- -provably solution of $\underline{\mathcal{C}}(e)$ with principal value e .

Proof. Immediate consequence of Lem. 3.4. ◀

► **Lemma** (= Lem. 6.2). Let $e, f, g \in \text{StExp}(A)$ with $f \downarrow$, and let $\Gamma := \{e = f \cdot e + g\}$. Then the star expression e is the principal value of a $(\text{Mil}^- + \Gamma)$ -provable solution of the 1-chart interpretation $\underline{\mathcal{C}}(f^* \cdot g)$ of $f^* \cdot g$.

Proof of Lemma 6.2 (extension of the proof on p. 15). First, it can be verified that the vertices of $\underline{\mathcal{C}}(f^* \cdot g)$ are of either of three forms:

$$V(\underline{\mathcal{C}}(f^* \cdot g)) = \{f^* \cdot g\} \cup \{(F * f^*) \cdot g \mid F \in \hat{\varrho}^+(f)\} \cup \{G \mid G \in \hat{\varrho}^+(g)\}, \quad (\text{A.2})$$

where $\hat{\varrho}^+(f)$ means the set of iterated 1-derivatives of f according to the TSS in Def. 3.2.

This facilitates to define a function $s : V(\underline{\mathcal{C}}(f^* \cdot g)) \rightarrow \text{StExp}(A)$ on $\underline{\mathcal{C}}(f^* \cdot g)$ by:

$$\begin{aligned} s(f^* \cdot g) &:= e, \\ s((F * f^*) \cdot g) &:= \pi(F) \cdot e, \quad (\text{for } F \in \hat{\varrho}^+(f)), \\ s(G) &:= \pi(G) \quad (\text{for } G \in \hat{\varrho}^+(g)), \end{aligned}$$

We will show that s is a $(\text{Mil}^- + \Gamma)$ -provable solution of $\underline{\mathcal{C}}(f^* \cdot g)$. Instead of verifying the correctness conditions for s for list representations of transitions, we will argue more loosely

16:22 A Coinductive Version of Milner's Proof System

with sums over action 1-derivatives sets $\underline{A\hat{\partial}}(H)$ of stacked star expressions H where such sums are only well-defined up to ACI. Due to $\text{ACI} \subseteq \text{Mil}^-$ such an argumentation is possible. Specifically we will demonstrate, for all $E \in V(\underline{\mathcal{C}}(f^* \cdot g))$, that s is a $(\text{Mil}^- + \Gamma)$ -provable solution at E , that is, that it holds:

$$s(E) \equiv_{(\text{Mil}^- + \Gamma)} \tau_{\underline{\mathcal{C}}(E)}(E) + \sum_{\langle \underline{a}, E' \rangle \in \underline{A\hat{\partial}}(E)} \underline{a} \cdot s(E'), \quad (\text{A.3})$$

where by the sum on the right-hand side we mean an arbitrary representative of the ACI equivalence class of star expressions that can be obtained by the sum expression of this form.

For showing (A.3), we distinguish the three cases of vertices $E \in V(\underline{\mathcal{C}}(f^* \cdot g))$ according to (A.2), that is, $E \equiv f^* \cdot g$, $E \equiv (F \star f^*) \cdot g$ for some $F \in \hat{\partial}^+(f)$, and $E \equiv G$ for some $G \in \hat{\partial}^+(g)$.

In the first case, $E \equiv f^* \cdot g$, we have argued on page 16 that s is a $(\text{Mil}^- + \Gamma)$ -provable solution at E , and hence that (A.3) holds for E as chosen here.

In the second case we consider $E \equiv (F \star f^*) \cdot g \in V(\underline{\mathcal{C}}(f^* \cdot g))$. Then $\tau_{\underline{\mathcal{C}}(E)}(E) \equiv \tau_{\underline{\mathcal{C}}((F \star f^*) \cdot g)}((F \star f^*) \cdot g) \equiv 0$ holds, because expressions with stacked products occurring do not have immediate termination by Def. 3.2. We distinguish the subcases $F \downarrow$ and $F \downarrow$.

For the first subcase we assume $F \downarrow$. Then $\tau_{\underline{\mathcal{C}}(F)}(F) \equiv 0$ holds, and we find by Lem. A.3 (or by inspecting the TSS in Def. 3.2):

$$\underline{A\hat{\partial}}((F \star f^*) \cdot g) = \{ \langle \underline{a}, (F' \star f^*) \cdot g \rangle \mid \langle \underline{a}, F' \rangle \in \underline{A\hat{\partial}}(F) \}. \quad (\text{A.4})$$

Now we argue as follows:

$$\begin{aligned} s(E) &\equiv s((F \star f^*) \cdot g) && \text{(in this case)} \\ &\equiv \pi(F) \cdot e && \text{(by the definition of } s) \\ &\equiv_{\text{Mil}^-} \left(\tau_{\underline{\mathcal{C}}(F)}(F) + \sum_{\langle \underline{a}, F' \rangle \in \underline{A\hat{\partial}}(F)} \underline{a} \cdot \pi(F') \right) \cdot e && \text{(by Lem. A.5)} \\ &\equiv_{\text{Mil}^-} 0 \cdot e + \sum_{\langle \underline{a}, F' \rangle \in \underline{A\hat{\partial}}(F)} \underline{a} \cdot (\pi(F') \cdot e) && \text{(by } \tau_{\underline{\mathcal{C}}(F)}(F) \equiv 0, \text{ due to } F \downarrow, \text{ and} \\ &&& \text{axioms (r-distr}(+, \cdot), \text{ (assoc}(\cdot))) \\ &\equiv_{\text{Mil}^-} 0 + \sum_{\langle \underline{a}, F' \rangle \in \underline{A\hat{\partial}}(F)} \underline{a} \cdot s((F' \star f^*) \cdot g) && \text{(by ax. (deadlock) and def. of } s) \\ &\equiv_{\text{ACI}} \tau_{\underline{\mathcal{C}}((F \star f^*) \cdot g)}((F \star f^*) \cdot g) + \sum_{\langle \underline{a}, E' \rangle \in \underline{A\hat{\partial}}((F \star f^*) \cdot g)} \underline{a} \cdot s(E') && \text{(due to (A.4), and } \tau_{\underline{\mathcal{C}}(E)}(E) \equiv 0) \\ &\equiv \tau_{\underline{\mathcal{C}}(E)}(E) + \sum_{\langle \underline{a}, E' \rangle \in \underline{A\hat{\partial}}(E)} \underline{a} \cdot s(E') && \text{(in this case).} \end{aligned}$$

For the second subcase we assume $F \downarrow$. Then $F \in \text{StExp}(A)$ (that is, F does not contain a stacked product symbol), and $\tau_{\underline{\mathcal{C}}(F)}(F) \equiv 1$ holds. Furthermore, we find, again by inspecting the TSS in Def. 3.2:

$$\underline{A\hat{\partial}}((F \star f^*) \cdot g) = \{ \langle 1, f^* \cdot g \rangle \} \cup \{ \langle \underline{a}, (F' \star f^*) \cdot g \rangle \mid \langle \underline{a}, F' \rangle \in \underline{A\hat{\partial}}(F) \}. \quad (\text{A.5})$$

Now we argue as follows:

$$\begin{aligned} s(E) &\equiv s((F \star f^*) \cdot e) && \text{(in this case)} \\ &\equiv \pi(F) \cdot e && \text{(by the definition of } s) \\ &\equiv_{\text{Mil}^-} \left(\tau_{\underline{\mathcal{C}}(F)}(F) + \sum_{\langle \underline{a}, F' \rangle \in \underline{A\hat{\partial}}(F)} \underline{a} \cdot \pi(F') \right) \cdot e && \text{(by Lem. A.5)} \end{aligned}$$

$$\begin{aligned}
&=_{\text{Mil}^-} 1 \cdot e + \sum_{\langle \underline{a}, F' \rangle \in \underline{A\hat{\rho}}(f)} \underline{a} \cdot (\pi(F') \cdot e) && \text{(by } \tau_{\underline{\mathcal{C}}(F)}(F) \equiv 1, \text{ and} \\
&&& \text{axioms (r-distr}(+, \cdot), \text{ (assoc}(\cdot))) \\
&\equiv 1 \cdot s(f^* \cdot g) + \sum_{\langle \underline{a}, F' \rangle \in \underline{A\hat{\rho}}(f)} \underline{a} \cdot s((F' \star f^*) \cdot g) && \text{(by the definition of } s) \\
&=_{\text{ACI}} 0 + \sum_{\langle \underline{a}, E' \rangle \in \underline{A\hat{\rho}}((F \star f^*) \cdot g)} \underline{a} \cdot s(E') && \text{(by (A.5), using axioms} \\
&&& \text{(comm}(+), \text{ and (assoc}(+))) \\
&\equiv \tau_{\underline{\mathcal{C}}(E)}(E) + \sum_{\langle \underline{a}, E' \rangle \in \underline{A\hat{\rho}}(E)} \underline{a} \cdot s(E') && \text{(in this case, due to } \tau_{\underline{\mathcal{C}}(E)}(E) \equiv 0).
\end{aligned}$$

Due to $\text{ACI} \subseteq \text{Mil}^- \subseteq \text{Mil}^- + \Gamma$, the chains of equalities in both subcases are provable in $\text{Mil}^- + \Gamma$, and therefore we have verified (A.3) also in the second case.

In the final case, $E = G$ for some $G \in \hat{\rho}^+(g)$, we argue as follows:

$$\begin{aligned}
s(E) &\equiv s(G) && \text{(in this case)} \\
&\equiv \pi(G) && \text{(by the definition of } s) \\
&=_{\text{Mil}^-} \tau_{\underline{\mathcal{C}}(G)}(G) + \sum_{\langle \underline{a}, G' \rangle \in \underline{A\hat{\rho}}(G)} \underline{a} \cdot \pi(G') && \text{(by Lem. A.5)} \\
&=_{\text{ACI}} \tau_{\underline{\mathcal{C}}(G)}(G) + \sum_{\langle \underline{a}, G' \rangle \in \underline{A\hat{\rho}}(G)} \underline{a} \cdot s(G') && \text{(by the definition of } s) \\
&=_{\text{ACI}} \tau_{\underline{\mathcal{C}}(E)}(E) + \sum_{\langle \underline{a}, E' \rangle \in \underline{A\hat{\rho}}(E)} \underline{a} \cdot s(E') && \text{(in this case).}
\end{aligned}$$

Due to $\text{ACI} \subseteq \text{Mil}^- \subseteq \text{Mil}^- + \Gamma$, this chain of equalities verifies (A.3) also in this case.

By having established (A.3) for the, according to (A.2), three possible forms of stacked star expressions that are vertices of $\underline{\mathcal{C}}(f^* \cdot g)$, we have established that s is indeed a $(\text{Mil}^- + \Gamma)$ -provable solution of $\underline{\mathcal{C}}(f^* \cdot g)$. ◀