On Orthogonality of Self-Distributivity

master thesis in computer science

by

Raoul Jasper Schikora

submitted to the Faculty of Mathematics, Computer Science and Physics of the University of Innsbruck

in partial fulfillment of the requirements for the degree of Master of Science

supervisors: Dr. Vincent van Oostrom,
assoc. Prof. Dr. René Thiemann
Department of Computer Science

Innsbruck, 1 November 2022

Master Thesis

On Orthogonality of Self-Distributivity

Raoul Jasper Schikora (11816400)
raoul.schikora@student.uibk.ac.at

1 November 2022

Supervisors: Dr. Vincent van Oostrom
assoc. Prof. Dr. René Thiemann

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides statt durch meine eigenhändige Unterschrift, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Alle Stellen, die wörtlich oder inhaltlich den angegebenen Quellen entnommen wurden, sind als solche kenntlich gemacht.
Die vorliegende Arbeit wurde bisher in gleicher oder ähnlicher Form noch nicht als Magister-/Master-/Diplomarbeit/Dissertation eingereicht.

Datum	Unterschrift

Abstract

This master thesis proves orthogonality of self-distributivity in the sense of having a residual system. Considering orthogonality in an advanced manner generalizing the purely syntactic definition was already done by Melliès [16] and by Terese [23, Chapter 8.7]. We pick up their approaches and first survey constructions of residual systems for left-linear and non-ambiguous term rewriting, for associativity and for braids. We then transfer established findings to self-distributivity. Furthermore, we generalize a statement about scopic relations from Melliès [17] as it is too restrictive for our purposes.

Contents

1 Introduction

Orthogonality describes left-linearity paired with non-ambiguity and provides a simple and syntactic notion ensuring the in general undecidable property of confluence. However, the concept is very restrictive. Nevertheless, a number of authors relax the conditions and allow special cases of ambiguity without jeopardizing confluence and consider orthogonality from a semantic point of view. Among others this is done by Melliès in an axiomatic approach [16] and in Terese via residual systems [23, Chapter 8.7], both allowing a notion of least common reduct. Van Oostrom showed that the former is an instance of the latter [25]. We pick up van Oostrom's findings and show in this master thesis that self-distributivity is orthogonal in the advanced, semantic sense.

Self-distributivity states that a binary operation $*$ distributes over itself and is for example described by the following equation[1]

$$(x * y) * z = (x * z) * (y * z). \tag{RD}$$

Self-distributive structures can be found in various fields. Three of the simplest structures are the logical operations of $\wedge, \vee$ and the geometrical interpretation of middle. In topology shelves, racks and quandles are defined via self-distributivity, which gained increasing interest since the early 2000s for example examined by Carter et al. [5, 6, 7] and Inoue & Kabaya [13]. Furthermore, Dehornoy showed in his monograph a close proximity to braids and studies the equational theory of RD [8]. Since the *Substitution Lemma* [23, Lemma 10.1.10] can be interpreted as an instance of RD, self-distributivity plays a key role to Tait and Martin-Löf's parallel β-step, which was refined by Takahashi and proves confluence of β-reducitons in λ-calculus [22].

Turning the RD-equation into a rewrite step orienting it in length increasing direction we obtain a term rewrite system consisting of a single rule. Undoubtedly, this system is ambiguous. This can already be seen from the term $((w*x)*y)*z$ as we can apply the rule either to the whole term or to the sub-term $(w*x)*y$. Hence, self-distributivity certainly does not fall under the syntactic notion of orthogonality. To still prove orthogonality under the semantic consideration we wish to proceed analogously to the *Parallel Moves Lemma* [23, Lemma 4.3.3], namely skolemising the diamond property of many-steps under a notion of least. Finding such a witnessing function of the skolemisation is in many cases non-trivial. A framework is given by Terese's residual systems in a way that a skolem function satisfying their residual identities is ensured to be a least upper bound.

We approach the problem of finding a suitable residual system by approximating it via three different constructions each on their own essentially easier, but still similar to self-distributivity: First, the S-combinator of combinatory logic also comprising duplication,

[1] The naming RD originates from *right* self-distributivity. However, with $x * (y * z) = (x * y) * (x * z)$ a symmetric *left* version exists.

second, associativity consisting of the same self-overlap, and third, braids showing a close proximity to self-distributivity. The former represents an orthogonal system in the syntactic as well as in the semantic interpretation. The latter two on the other hand are only orthogonal from the semantic perspective.

One common building block of the former two mentioned methods are proof terms providing convenient representations of reduction sequences allowing a compact, inductive perspective. Another important role and a common denominator between braids and self-distributivity play Melliès' scopic relations formalizing a dual concept to transitivity [17].

Related Work

Confluence of self-distributivity is already proven by van Oostrom [27]. Contrary to the approach in the present thesis, this is done via a least upper bound for all, instead of for only two single steps having the same source. This procedure goes back to Dehornoy established in his monograph on self-distributivity [8]. This monograph also explains the connection between self-distributivity and braids.

Further studies of braids are done by Endrullis & Klop [10]. The foundation to the modern understanding of braids made Artin discretizing their continuous notion [1].

Proof terms formalize Meseguers rewriting logic [18] and were used by van Oostrom and de Vrijer in Terese to show equivalences of reductions [23, Chapter 8], which can also be found in excerpts in a corresponding research article [28].

The terminology of a scopic relation emerged from Melliès [17], however, the characterization in general goes back to Guilbaud & Rosenstiehl studying combinatorial properties of permutations [20].

Basics of rewriting are covered by Baader & Nipkow [2], and in Terese [23]. The latter also provides most of the basis to this thesis. Some more advanced topics are dealt with by Ohlebusch [19].

An introduction to λ-calculus can be found in Terese [23, Chapter 10] and a thorough survey is given by Barendregt [3].

Fundamentals of order theory provides, e.g., the textbook by Hein also explaining skolemisation [11]. Least upper bounds and the strongly connected (semi)-lattices are, among many others studied by Burris & Sankappanavar, where also the connection from the order theoretical to the universal algebraic approach are demonstrated [4].

Structure of Present Text

The second chapter provides a collection of preliminaries necessary to understand this thesis. It mainly recapitulates required concepts or gives references to them, introduces notation and proves some lesser known but important statements for later findings. It is divided into three parts, where the first is concerned with discrete mathematics and, where the second and the third are dedicated to rewriting including the syntax and semantics of terms. Readers familiar with either of the topics may only scan through the respective section or even skip it completely and only come back to it when needed.

The subsequent chapter considers a dual of transitivity called scopicness. For the most part it generalizes a result stated by Melliès [17], as the theory established by him is developed under assumptions too strong for our purposes becoming important in Chapter 6.

Chapter 4 is meant to introduce residual systems. Firstly, proof terms are defined and it is shown that they indeed equal reductions. Furthermore, overlaps are investigated and the syntactic notion of orthogonality is defined. Additionally, tracing and trace algebras are established, which we will use later as models for the diamonds. Lastly, residual systems are presented and the connection to the diamond property is demonstrated.

Chapter 5 puts residuation to action and collects some comprehensive examples suggesting that the witness function is not always obvious to find. Moreover, we collect certain insights we will be taking to the next section.

Chapter 6 applies the preceding findings to self-distributivity. The initial section explains the setting used and shows local-confluence of the established system followed by a section showing the system's completeness. At last, we provide a witnessing function skolemising the diamond property and prove its residual attributes.

We end with a conclusion and an outlook on future work to an inductive approach of self-distributivity.

In the following git-repository a code base on orthogonality of self-distributivity can be found, which can be used to generate examples and calculate residuals:

`https://git.uibk.ac.at/csav8467/orthogonality_of_self-distributivity`

2 Preliminaries

The following chapter is meant to set the basis from where succeeding chapters will start and ensure that the reader and the author have the same understanding of the fundamental concepts necessary for this thesis. Many notions are not elaborated in detail but only referenced. The first section is related to concepts from discrete mathematics, whereas the second section focuses on abstract rewriting and the third section on term rewriting.

2.1 Sets, Relations and Orders

The fundamentals of this thesis are provided by discrete mathematics. If not stated otherwise we adopt definitions and notations concerning sets, relations and orders from Hein as in [11]. Throughout this thesis we will, moreover, consider binary endorelations, i.e., by a relation R we always mean a binary relation on $X \times X$ for some set X. Furthermore, we will use the following notation.

Notation 2.1.1. For a relation R over $X \times X$ we denote by R^{-1} the *converse* relation, i.e. $R^{-1} = \{(a,b) \mid (b,a) \in R\}$. In addition, we define

$$(a\ R) := \{b \mid a\ R\ b\}$$
$$(S\ R) := \bigcup_{a \in S} (a\ R)$$

for an element $a \in X$ and a set $S \subseteq X$.

In the context of braids we will encounter a binary operation on relations representing a step. Melliès called this operation an addition and we will adopt his terminology [17]. It replaces elements of the first relation by the corresponding elements of the second's converse relation.

Definition 2.1.2. The *addition* of two binary relations R, S on the same set X is defined as

$$R + S := (R - S) \cup S^{-1}.$$

However, note that the addition on relations is neither commutative nor associative. Furthermore, the addition is not left neutral.

Often we will consider paths in binary relations. This will be done according to Hein interpreting a binary relation as a directed graph [11]. Then, a path is a sequence of edges, also determining its length, that we can denote by a sequence of vertices, allowing the notion of distances between elements of a binary relation.

Definition 2.1.3. The *distance* of two elements $a, c \in X$ in a relation R over $X \times X$ is defined as the distance in the corresponding directed graph G, where the distance of two distinct vertices v, w is defined as the minimal length over all paths starting in v and ending in w, if no such path exists in G the distance is defined to be ∞, the distance of v to v is defined as 0.

The distance of two elements in a relation becomes important when proving properties of a dual notion to transitive relations in Chapter 3. Actually, transitivity will be a concept accompanying the reader throughout the whole course of this thesis. Especially, for a binary relation R we will be interested in the smallest transitive relation that contains R. This matches exactly the definition of transitive closure from Hein [11], which we will be denoting by R^+. As it is often convenient to argue with the closure properties of R^+, we show in the following that the transitive closure is a closure operator defined in the sense of Burris & Sankappanavar [4].

Definition 2.1.4. A mapping $C : 2^X \to 2^X$ is called a *closure operator* on X, if for $R, S \subseteq X$ it satisfies:

- $R \subseteq C(R)$ *(extensive)*
- $C(C(R)) = C(R)$ *(idempotence)*
- $S \subseteq R$ implies $C(S) \subseteq C(R)$ *(monotone, isotone or increasing),*

where 2^X denotes the power set of X.

Remark 2.1.5. To see that the transitive closure is a closure operator in the sense of Definition 2.1.4, note that extensiveness and idempotence are obvious. To see monotonicity, assume that $S \subseteq R$ and $S^+ \nsubseteq R^+$, then as transitivity is closed under intersection there exists a transitive proper subset $T \subset S^+ \cap R^+$ with $S \subseteq T$, which contradicts the definition of S^+ being the smallest transitive set containing S.

For a construction of the transitive closure we refer again to Hein [11]. Furthermore, we will take advantage of the transitive reduct of a transitive relation, which is the corresponding binary relation to the graph also known as the *Hasse* diagram. From the transitive reduct we can construct the irreflexive part of the initial transitive relation by the transitive closure. A partial order can be reconstructed by the reflexive–transitive closure of its transitive reduct.

Definition 2.1.6. Let R be a transitive relation. Define the *transitive reduct* of R as the relation

$$r(R) := \{(a, b) \mid a \text{ is an immediate predecessor of } b\},$$

where a is an immediate predecessor of b, if $\{\ c \in X \mid a\ R\ c\ R\ b\ \} = \emptyset$ and $a \neq b$.

An essential part of our to be established characterization of Chapter 6 relies on the concept of prefix orders, that intuitively speaking generalize the idea of trees and have the convenient property of uniqueness of paths in their transitive reduct.

Definition 2.1.7. A *prefix order* is a reflexive, transitive and anti-symmetric relation $\sqsubseteq$, i.e., a partial order, such that $a \sqsubseteq b \ \wedge\ c \sqsubseteq b$ implies $a \sqsubseteq c \ \vee\ c \sqsubseteq a$. A *strict prefix order* $\sqsubset$ is the irreflexive part of a prefix order $\sqsubseteq$.

Lemma 2.1.8. *Paths in the transitive reduct of a prefix order are unique.*

Proof. Let $\sqsubseteq$ be a prefix order and assume there exist two distinct paths P, Q from a to b in X in the transitive reduct of $\sqsubseteq$. Let $x \in X$ be the first element, where P and Q divert. Hence, there exist $y, z \in X$, such that x is an immediate predecessor of y and of z according to $\sqsubseteq$, and moreover, without loss of generality, $x \sqsubseteq y$ is an edge in P but not in Q and, vice versa, $x \sqsubseteq z$ is an edge in Q but not in P. However, $z \sqsubseteq b \ \wedge\ y \sqsubseteq b$, which implies by $\sqsubseteq$ being a prefix order $y \sqsubseteq z \ \vee\ z \sqsubseteq y$. Assume the former, i.e., $x \sqsubseteq y \sqsubseteq z$, contradicting x being an immediate predecessor of z. Proceed symmetrically for the latter. ☐

We now turn our attention back to the transitive closure and related observations. Firstly, we state an easy consequence resulting from the closure properties, which is however an important insight for what is about to follow.

Lemma 2.1.9. *Let R be a transitive relation and $S \subseteq R$, then $S^+ \subseteq R$.*

Proof. From $S \subseteq R$ it follows that $S^+ \subseteq R^+$ by $+$ being a closure operator. Since R is transitive $R = R^+$ and, hence, $S^+ \subseteq R$. ☐

The problems arising concerning the comprehensive example of braids in the end boil down to two set theoretic properties related to the transitive closure. The proof to the first one goes back to Klop et al. [15, Proposition 32]. For the sake of completeness we recapitulate it here.

Lemma 2.1.10. *Let $S, T, U \subseteq R$ be transitive relations with $R - U \in S \cap T$, then $(U \cap (S \cup T))^+ = U \cap (S \cup T)^+$.*

Proof. Since transitive relations are closed under intersection, obviously $U^+ \cap (S \cup T)^+$ is transitive, hence, from $U \cap (S \cup T) \subseteq U^+ \cap (S \cup T)^+$ follows $(U \cap (S \cup T))^+ \subseteq U^+ \cap (S \cup T)^+ = U \cap (S \cup T)^+$ by Lemma 2.1.9 and transitivity of U.

To prove $U \cap (S \cup T)^+ \subseteq (U \cap (S \cup T))^+$ we show by induction that for each $m \in \mathbb{N}$ it holds that $a\, U\, b$ and $a\ (S \cup T)^m\ b$ implies $a\ (U \cap (S \cup T))^+\ b$. Choose m to be minimal. For $m = 1$ the claim trivially holds. Let $m > 1$ and $a\ (S \cup T)^{m_1}\ c \ \wedge\ c\ (S \cup T)^{m_2}\ b$ for some c and $1 \leq m_1, m_2 < m$. Furthermore, assume $a\ (R - U)\ c$, hence, by condition of the statement to be proven $a\ (S \cap T)\ c$ and by S, T being transitive it follows $a\ (S \cup T)^{m_2}\ b$. Thus, contradicting m being minimal it holds that $a\, U\, c \ \wedge\ a\ (S \cup T)^{m_1}\ c$. Similarly, it holds that $c\, U\, b \ \wedge\ c\ (S \cup T)^{m_2}\ b$. Consequently, $a\ (U \cap (S \cup T))^+\ b$. ☐

The second of the afore-mentioned set theoretic properties is the equality of $(S \cup (T \cup U)^+)^+ = (S \cup T \cup U)^+$ for relations $S, T, U \subseteq R$, which is an instance of the next lemma.

Lemma 2.1.11. *Let $S, T \subseteq R$ be relations, then $(S \cup T^+)^+ = (S \cup T)^+$.*

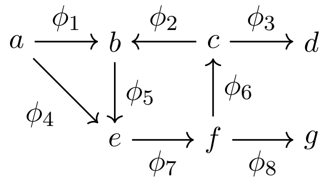


Figure 2.1: Example of an ARS.

Proof. The inclusion $(S \cup T)^+ \subseteq (S \cup T^+)^+$ holds by monotonicity of closure operators, since $T \subseteq T^+$. To see that the reverse inclusion also holds, note that by definition of closure operator $S \subseteq S^+ \subseteq (S \cup T)^+$ and, similarly, $T^+ \subseteq (S \cup T)^+$, since $S, T \subseteq S \cup T$. Consequently, $S \cup T^+ \subseteq (S \cup T)^+$. Once more by definition of closure operator it follows that $(S \cup T^+)^+ \subseteq ((S \cup T)^+)^+ = (S \cup T)^+$. $\square$

2.2 Abstract Rewriting

For most rewriting purposes it suffices to be able to express *whether or not* two objects are related by a step. For this reason an *abstract rewriting system* is often defined as a relation (e.g., see [23, Definition 1.1.1]). However, in the theory of residuation it is desirable to express *what* step relates two objects to another, as the objects of interest are residuals of steps, thus, steps having an identity is useful. Henceforth, we define an abstract rewrite system via steps.

Definition 2.2.1. An *abstract rewrite system* (ARS) is a quadruple $\langle A, \Phi, \mathrm{src}, \mathrm{tgt} \rangle$ with A a set of *objects*, Φ a set of *steps* and $\mathrm{src}, \mathrm{tgt} : \Phi \to A$ the *source* and *target* function, i.e., for a step ϕ there exists $a, b \in A$ such that $a \overset{\mathrm{src}}{\leftarrow} \phi \overset{\mathrm{tgt}}{\rightarrow} b$.

Two steps ϕ, ψ are called *co-initial*, if $\mathrm{src}(\phi) = \mathrm{src}(\psi)$. They are called *composable*, if $\mathrm{tgt}(\phi) = \mathrm{src}(\psi)$. They are called *co-final*, if $\mathrm{tgt}(\phi) = \mathrm{tgt}(\psi)$.

Remark 2.2.2. In Definition 2.2.1 steps are first class citizens of the ARS serving the purpose to distinguish *what rule* relates source and target. In what follows we may use various arrow-like symbols, such as $\to, \rightarrowtail, \geq, \ldots$ to denote an ARS and often write $\phi : a \to b$, where the step ϕ with src-, and tgt-function resulting in a and b of the ARS $\to$ is meant, respectively. However, we will not limit ourself to this notation and also use mixed versions such as $\phi \in R$ or $\phi : a \to b \in R$ for steps in an ARS R. In figures we will also use $a \xrightarrow{\phi} b$.

Example 2.2.3. Let $A = \{a, b, c, d, e, f\}$ be a set of objects and $\Phi = \{\phi_1, \ldots, \phi_8\}$ a set of steps, such that $\phi_1 : a \to b, \phi_2 : c \to b, \phi_3 : c \to d, \phi_4 : a \to e, \phi_5 : b \to e, \phi_6 : f \to c, \phi_7 : e \to f$ and $\phi_8 : f \to g$ define the src- and tgt-function, see Figure 2.1. Then, $\to := \langle A, \Phi, \mathrm{src}, \mathrm{tgt} \rangle$ defines an ARS.

Remark 2.2.4. The afore-mentioned relational view usually defines an ARS as a tuple $(A, \to)$ consisting of a set A and a binary relation $\to$ on A. This can easily be expressed in terms of the Definition 2.2.1 by $(A, \{\to_\phi \mid \phi \in \Phi\})$, where $\to_\phi$ relates the source and the target of the step ϕ.

On the other hand, for a given relation $\to$ on A we can index the elements in $\to$ by an index set I, such that each element $(a,b) \in \to$ has a unique index $i \in I$ and denote this by $(a,b)_i$. Then $\langle A, \{(a,b)_i \mid i \in I, a, b \in A\}, \mathrm{src}, \mathrm{tgt}\rangle$ with $\mathrm{src}((a,b)_i) = a$ and $\mathrm{tgt}((a,b)_i) = b$ defines an ARS in the sense of Definition 2.2.1.

The above remark shows the equivalence of the relational view on ARS to that considering steps as first class citizens. Therefore, we can easily switch between views by translating accordingly. However, this thesis develops the theory corresponding to Definition 2.2.1 and for the remainder of this section the most important concepts used in later sections are introduced. The reader familiar with term rewriting can safely skip to Chapter 3 without missing established content.

An important property throughout this work is the diamond property expressing the existence of two co-final steps for two co-initial steps.

Definition 2.2.5. Two co-initial steps $\phi : s \to t_1, \psi : s \to t_2$ fulfil the *diamond property*, if there exist two co-final steps $\phi' : t_1 \to t, \psi' : t_2 \to t$. An ARS admits the *diamond property*, if for all pairs of co-initial steps the diamond property holds.

As we are interested in the diamond property of *many-steps*, we suitably supplement ARS's by the notion of composition.

Definition 2.2.6. An abstract rewrite system with *composition* is a triple $\langle \to, 1, \cdot \rangle$, where $\to$ is an ARS, 1 a function from objects to steps, and $\cdot$ a function from composable steps to steps, such that:

- For every object a, its trivial step $1_a : a \to a$ exists.
- For every pair of composable steps $\phi : a \to b, \psi : b \to c$, their composition $\phi \cdot \psi : a \to c$ exists.

Furthermore, we want to be able to consider an equivalent to what in the relational point of view is done via the reflexive-transitive closure, namely, a reduction sequence of length 0 or more.

Definition 2.2.7. The *reflexive-transitive closure* $\to^*$ of an ARS $\to := \langle A, \Phi, \mathrm{src}, \mathrm{tgt}\rangle$ is the ARS with composition defined by:

- A is the set of objects.
- the steps together with their source and target are defined by the following inference rules:

$$\frac{a \in A}{1_a : a \to^* a} \qquad \frac{\phi : a \to b \in \Phi}{\phi : a \to^* b} \qquad \frac{\phi : a \to^* b \qquad \psi : b \to^* c}{(\phi \cdot \psi) : a \to^* c}$$

- The trivial step for an object a is $1_a : a \to^* a$.
- The composition of $\phi : a \to^* b$ and $\psi : b \to^* c$ is $(\phi \cdot \psi) : a \to^* c$.

Steps of the form 1_a will be called *empty* steps and we will often just write a or 1 to denote 1_a. Steps of the form $(\phi \cdot \psi)$ will be called *composite* steps.

However, this still does not quite do the job as, e.g., the composition $(\phi \cdot \psi) \cdot \chi$ is different from $\phi \cdot (\psi \cdot \chi)$ as well as $\phi \cdot 1$ is different from ϕ. To cope with that we simply quotient the monoid identities and associativity out. This is what we then call a reduction.

Definition 2.2.8. Let $\to$ be an ARS. The ARS $\twoheadrightarrow$ is the ARS resulting from $\to^*$ modulo the monoid identities $\phi \cdot 1 \approx \phi$, $1 \cdot \phi \approx \phi$ and $(\phi \cdot \psi) \cdot \chi \approx \phi \cdot (\psi \cdot \chi)$. A step $\phi : s \twoheadrightarrow t$ is also called a *reduction*.

Hence, due to associativity we may omit parenthesis in compositions, when we consider reductions.

By the nature of rewriting it is always favourable to consider complete systems, as their canonical structure makes life easier and, which is what we will consequently strive for in Chapter 5 and 6. Next the meaning of complete rewrite system and the essentially related notions confluence and normalization are repeated. Furthermore, we present increasing ARS's, which play an important role on the path to the main theorem of Chapter 6. Example 2.2.10 and 2.2.14 illustrate these properties.

Definition 2.2.9. Let $\to := \langle A, \Phi, \mathrm{src}, \mathrm{tgt} \rangle$ be an ARS. An element $s \in A$ is called

- *locally confluent*, if for any steps $\phi, \psi \in \Phi$ with $\phi : s \to t_1$ and $\psi : s \to t_2$, there exist reductions ϕ', ψ' of $\to$ such that $\phi' : t_1 \twoheadrightarrow t$ and $\psi' : t_2 \twoheadrightarrow t$ for some $t \in A$.
- *confluent*, if for any two reductions ϕ, ψ of $\to$ with $\phi : s \twoheadrightarrow t_1, \psi : s \twoheadrightarrow t_2$, there exist co-final reductions ϕ', ψ', i.e., there exists an object $t \in A$ such that $\phi' : t_1 \twoheadrightarrow t, \psi' : t_2 \twoheadrightarrow t$.
- a *normal form*, if for all $a \in A$ there exists no step $\phi \in \Phi$, such that $\phi : s \to a$.
- *weakly normalizing*, if there exists a normal form n and a reduction ϕ of $\to$, such that $\phi : s \twoheadrightarrow n$.
- *strongly normalizing* or *terminating*, if there are no infinite rewrite sequences starting in s, i.e., if there exists no infinite family $\{\phi_n \mid n \in \mathbb{N}\}$ of steps starting with ϕ_0 and ϕ_n composable with ϕ_{n+1}, such that $\mathrm{src}(\phi_0) = s$.

We call an ARS *locally confluent* (*confluent*, *weakly normalizing*, *strongly normalizing* or *terminating*), if all elements in A are locally confluent (confluent, weakly normalizing, strongly normalizing or terminating).

In addition, an ARS is *complete*, if it is confluent and terminating. An ARS $\to$ is *increasing*, if there exists a function $|\,.\,| : A \to \mathbb{N}$, such that for all $\phi : s \to t \in \Phi$ it holds that $|s| < |t|$.

Example 2.2.10. Consider the ARS $\to$ of Example 2.2.3. The normal forms of $\to$ are d and g. The ARS $\to$ is locally confluent as for any co-initial steps there exist co-final reductions. However, since from every object there exist reductions to both normal forms, no element is confluent except for the normal forms themselves. For the same reason the ARS is weakly normalizing. However, it is not terminating as we can infinitely often compose $\phi_2 \cdot \phi_5 \cdot \phi_7 \cdot \phi_6 : c \to c$.

In various sections we will be only interested in parts of an ARS and with the following definition this is formalized.

Definition 2.2.11. Let $\to_i := \langle A_i, \Phi_i, \mathrm{src}_i, \mathrm{tgt}_i \rangle$ be an ARS for $i \in \{1, 2\}$. We say $\to_1$ is a *sub-abstract-rewriting-system* (sub-ARS) of $\to_2$, denoted by $\to_1 \subseteq \to_2$, if $A_1 \subseteq A_2$, $\Phi_1 \subseteq \Phi_2$, and $\mathrm{src}_1, \mathrm{tgt}_1$ are the restrictions of $\mathrm{src}_2, \mathrm{tgt}_2$ to Φ_1.

An important application of sub-ARS makes use of the diamond property to show confluence by tiling the plane, which is expressed in the following proposition.

Proposition 2.2.12. *Let $\to, \rightarrowtail$ be ARSs, such that $\to \subseteq \rightarrowtail \subseteq \to^*$. If $\rightarrowtail$ has the diamond property, then $\to$ is confluent.*

Proof. An easy induction shows that for $\phi_1 \cdot \ldots \cdot \phi_n : s \rightarrowtail^* t_1$ and $\psi_1 \cdot \ldots \cdot \psi_m : s \rightarrowtail^* t_2$ we find $\phi'_1 \cdot \ldots \cdot \phi'_m : t_1 \rightarrowtail^* t$ and $\psi'_1 \cdot \ldots \cdot \psi'_n : t_2 \rightarrowtail^* t$ for $m, n \geq 0$ due to the diamond property. Replacing all steps of $\rightarrowtail$ by the corresponding compositions of $\to$ proves the claim. ☐

Another important use of sub-ARS are strategies. Intuitively, a strategy for an ARS narrows the options of possibilities down to a selection of steps, while the objects and normal forms stay untouched. Ideally this selection then has nicer properties from which we can draw conclusions on the initial ARS. This will be the approach on proving orthogonality in the semantic sense of self-distributivity. Thusly, strategies are defined and an example strategy is given afterwards.

Definition 2.2.13. A *strategy* for an ARS $\to$ is a sub-ARS $\to' \subseteq \to$ having the same set of objects and the same set of normal forms.

Example 2.2.14. Consider $\to$ of Example 2.2.3. Let $\Phi' = \{\phi_1, \phi_3, \phi_4, \phi_5, \phi_7, \phi_8\}$ and $\mathrm{src}', \mathrm{tgt}'$ the restrictions of src respectively tgt on Φ'. Then $\to' := \langle A, \Phi', \mathrm{src}', \mathrm{tgt}' \rangle$ is a sub-ARS of $\to$, see Figure 2.2. And, since $\to'$ consists of the same set of objects and has the same set of normal forms as $\to$ the sub-ARS $\to'$ also is a strategy for $\to$. Furthermore, the strategy $\to'$ is complete, as it is confluent and terminating.

In Chapter 6 the difficulty lies in proving termination of that chapter's rewrite system of interest. As already hinted above, this problem is approached by defining a terminating strategy. In consequence this means that the underlying ARS is weakly normalizing, and as it will also be shown to be locally confluent and increasing the following theorem ensures termination. Hence, what is about to come is one of the key ingredients to the main statement of Chapter 6. For the sake of importance and completeness the theorem

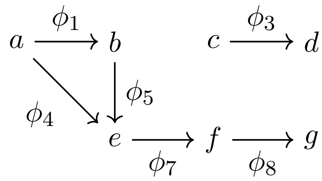


Figure 2.2: A corresponding strategy to the ARS of Example 2.2.3.

is proven here, but it may be mentioned that the proof is closely oriented on [23, Theorem 1.2.3 (iii)]. The reader unfamiliar with Newman's Lemma, stating that a terminating ARS is confluent if it is locally confluent, is referred to almost any relevant reference book on term rewriting, e.g., Baader & Nipkow [2, Lemma 2.7.2] or Terese [23, Theorem 1.2.1], as we will use it here without proof.

Theorem 2.2.15. *Let $\to$ be an ARS. If $\to$ is locally confluent, weakly normalizing and increasing, then $\to$ is also terminating.*

Proof. We prove the claim by contradiction. Let $\to := \langle A, \Phi, \mathrm{src}, \mathrm{tgt}\rangle$ be locally confluent, weakly normalizing and increasing. Moreover, let $a_1 \in A$ be non-terminating. Nonetheless, by weak normalization there exists an $a_n \in A$ and a composition $\phi_1 \cdot \ldots \cdot \phi_n : a_1 \twoheadrightarrow a_n$ with $\phi_i : a_i \to a_{i+1} \in \Phi$ for $1 \leq i \leq n-1$ such that a_n is a normal form. Obviously, a_n is terminating. Let a_k be non-terminating, such that $a_{k+1}, \ldots, a_n$ are terminating, i.e., a_k is the first non-terminating object starting from a_n backwards along the reduction defined by the composition $\phi_k \cdot \ldots \cdot \phi_n$. It follows that there exists an infinite family of successively composable steps $\psi_1 \cdot \psi_2 \cdot \ldots$ sourced at a_k, as a_k is not terminating. However, since $\to$ is locally confluent there exist co-final reductions ϕ', ψ' of the form $\phi' : a_{k+1} \twoheadrightarrow c, \psi' : b_1 \twoheadrightarrow c$, where $b_1 = \mathrm{tgt}(\psi_1)$. The sub-ARS consisting of the set A_{k+1} of all reachable elements from a_{k+1} together with the set of steps having a source in A_{k+1} (and the corresponding restrictions of the src- and tgt-function) is terminating, as a_{k+1} is terminating. With local confluence and Newman's Lemma the sub-ARS is also confluent, hence, there exist co-final reductions having c and a_n as source. As a_n is a normal form these reduction are of the form $\chi : c \twoheadrightarrow a_n$ and $1_{a_n} : a_n \twoheadrightarrow a_n$. As $\to$ is increasing the inequality $|a_1| \leq |a_k| < |b_1|$ holds. Inductively repeating the process for b_1 and a_n we find an unbounded sequence $|a_1| \leq |a_k| < |b_1| \leq |b_k| < \ldots$ contradicting the fact, that $|a_n|$ constitutes an upper bound. Consequently, $\to$ must be terminating (see Figure 2.3). □

2.3 Term Rewriting

For most parts of this thesis we are interested in term rewriting systems. As the name already suggests we are thus concerned with rewrites of terms. Due to the importance of a term we repeat its syntax here, but note that it is the standard notion also used by Baader & Nipkow [2, Definition 3.1.2] and Terese [23, Definition 2.1.2] under their

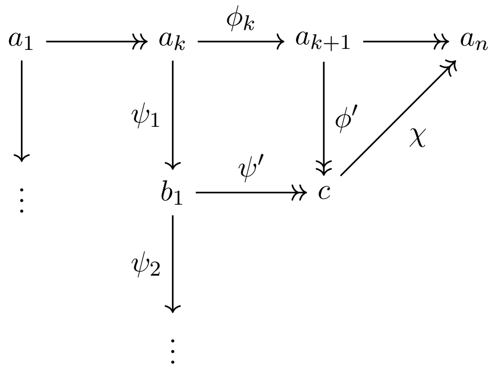


Figure 2.3: Proving termination of a locally confluent, weakly normalizing and increasing ARS by deriving a contradiction blowing up the path from a_1 to a_n.

usual definition of signature. Furthermore, we adopt the convention that $a, b, c, \ldots$ denote function symbols of arity zero (constants), $f, g, h, \ldots$ denote function symbols of higher arity and $z, y, x, \ldots$ denote variables.

Definition 2.3.1. For a signature Σ and an infinite set of variables $\mathcal{V}$ distinct from Σ we define the set $\mathcal{T}(\Sigma, \mathcal{V})$ as the smallest set such that $\mathcal{V} \subseteq \mathcal{T}(\Sigma, \mathcal{V})$ and $f(t_1, \ldots, t_n) \in \mathcal{T}(\Sigma, \mathcal{V})$ if the arity of f is n and $t_1, \ldots, t_n \in \mathcal{T}(\Sigma, \mathcal{V})$. If $t \in \mathcal{T}(\Sigma, \mathcal{V})$ we call t a *term*.

Terms not containing a variable are called *ground* terms. Terms in which no variable occurs more than once are called *linear*. The set $\mathcal{V}(t)$ denotes the set of variables in the term t.

A term can be represented as a tree via its internal structure by the following definition.

Definition 2.3.2. Let t be a term. The *term tree* of t is inductively defined as the tree consisting of a single node labelled by t, if t is a constant or variable, and as the tree having the symbol f as label and the trees representing $t_1, \ldots, t_n$ from left to right as immediate sub-trees, if $t = f(t_1, \ldots, t_n)$.

If not stated otherwise, we adopt definitions and notation from Terese [23] concerning term rewriting, especially regarding *sub-term*, *substitution*, *position* and *context*. For the convenience of the reader we repeat (and slightly extend) the most important notations here.

Notation 2.3.3. We denote by $\mathcal{P}os$ the set of positions, by $\mathcal{P}os(t)$ the set of all positions in the term t, for $P \subseteq \mathcal{P}os(t)$ we call P connected, if P is connected in the term tree of t and we say two positions p_1, p_2 are parallel if neither is a prefix of the other and write $p_1 \parallel p_2$. The set $\mathcal{P}os_\Sigma(t)$ defines the non-variable positions in the term t and $t|_p$ defines the sub-term of the term t at position p.

In addition, $C[t_1, \ldots, t_n]$ determines the result of replacing the holes in the context C from left to right by the terms $t_1, \ldots, t_n$. A *one-hole context* is denoted by $C[\ ]$ and if $t = C[s]$ for a context C and $t, s \in \mathcal{T}(\Sigma, \mathcal{V})$ the term s is called a sub-term of t. If

$t = D[C[t_1, \ldots, t_n]]$ for some context D and some terms $t_1, \ldots, t_n$ the context C is a *subcontext* or *slice* of t. If $t = C[s]$ for some terms t, s, the context $C[\ ]$ is also called a *prefix* of t.

Concerning positions we will often be interested in ordering them according to their prefix relation. Hence, from now on $\sqsubseteq$ defines the standard prefix order on positions, i.e., we will consider positions as the partially ordered set $\langle \mathcal{P}os, \sqsubseteq \rangle$. By $\sqsubset$ we denote the irreflexive part of $\sqsubseteq$.

Describing orthogonality of steps we fall back on function symbol occurrences, denoting a pair consisting of a function symbol and the context it appears in.

Definition 2.3.4. The ordered pair $\langle s \mid C[\ ] \rangle$ determines the unique *occurrence* of s in a term $t = C[s]$. The pair $\langle f \mid C[\ ] \rangle$ determines the unique *occurrence of the function symbol* f in the term $C[f(t_1, \ldots, t_n)]$ for some terms $t_1, \ldots, t_n$, i.e., the head-symbol of $f(t_1, \ldots, t_n)$.

Concerning associativity and self-distributivity we will not only be interested in syntactic properties but also give semantics to terms. This is done by means of a Σ-algebra.

Definition 2.3.5. Let Σ be a signature. A Σ-*algebra* $\mathfrak{A}$ is a tuple $(A, \{f_{\mathfrak{A}}\}_{f \in \Sigma})$, where A is a set and $f_{\mathfrak{A}} : A^n \to A$ an operation for the n-ary function symbol $f \in \Sigma$. The set A is called the carrier of the Σ-algebra and $f_{\mathfrak{A}}$ the *interpretation* of $f \in \Sigma$.

Moreover, we can evaluate a term, which we call an interpretation. For our purposes it suffices to only define this interpretation over ground terms. However, we note that this is a very brief introduction and refer for further details to relevant textbooks.

Definition 2.3.6. Let $\mathfrak{A}$ be an Σ-algebra. We inductively define the evaluation of ground terms by the function

$$[f(t_1, \ldots, t_n)]_{\mathfrak{A}} = f_{\mathfrak{A}}([t_1]_{\mathfrak{A}}, \ldots, [t_n]_{\mathfrak{A}}),$$

where the interpretation of a constant t is defined as $[t]_{\mathfrak{A}} = t_{\mathfrak{A}}$.

An omnipresent example represents the set of natural numbers together with a signature consisting of a nullary, unary and a binary function symbol.

Example 2.3.7. Consider the signature $\Sigma = \{\mathbf{0}, \mathbf{s}(\cdot), +(\cdot, \cdot)\}$. The interpretations $\mathbf{0}_{\mathfrak{A}} = 0$, $\mathbf{s}_{\mathfrak{A}}$ as the successor function and $+_{\mathfrak{A}}$ as addition on the carrier of the natural numbers $\mathbb{N}$ constitutes a Σ-algebra $\mathfrak{A}$.

Furthermore, the term $\mathbf{s}(\mathbf{s}(\mathbf{0}) + \mathbf{s}(\mathbf{s}((\mathbf{0})))$ is a ground term over the signature Σ and is interpreted as $\mathbf{s}_{\mathfrak{A}}\left(\mathbf{s}_{\mathfrak{A}}\left(\mathbf{0}_{\mathfrak{A}}\right) +_{\mathfrak{A}} \mathbf{s}_{\mathfrak{A}}\left(\mathbf{s}_{\mathfrak{A}}\left(\mathbf{0}_{\mathfrak{A}}\right)\right)\right) = ((0+1) + ((0+1)+1)) + 1 = 4$.

After a short digression on the semantics of terms we finally define a term rewriting system, which differs from the relational point of view in as much as rules carrying names. The benefit of naming rules becomes evident in Section 4.1 introducing proof terms.

Definition 2.3.8. A *term rewriting system* (TRS) is a tuple $(\Sigma, \to)$, such that Σ is a signature and $\to$ is an ARS having terms in $\mathcal{T}(\Sigma, \mathcal{V})$ as objects and rules as steps, where a step $\rho : \ell \to r$ is a *rule*, when $\ell \notin \mathcal{V}$ and $\mathcal{V}(r) \subseteq \mathcal{V}(\ell)$. The source of a rule is called its *left-hand side (lhs)* and the target is called its *right-hand side (rhs)*, respectively. A TRS is called *left linear*, if for each rule $\rho : \ell \to r$ the term ℓ is linear.

Note that for each TRS we associate an ARS. Steps of the associated ARS are defined via term rewriting. The act of term rewriting itself is as usual done by means of context and substitution, which we do not elaborate any further but only refer to the standard term rewriting literature as, e.g., Baader & Nipkow [2] or Terese [23]. Properties such as confluence, termination, et cetera are always obtained via the associated ARS. Also, we will often denote a TRS only by its rules. As an example of a left-linear TRS consider the following.

Example 2.3.9. Let $(\Sigma, \to)$ be a TRS with the rules $\rho : f(f(x)) \to x$ and $\varsigma : g(f(x), y) \to g(x, f(y))$. Then $(\Sigma, \to)$ is left-linear, as the left-hand sides are linear.

With the last theorem of this section we point out that confluence of a TRS is not an *easy* property.

Theorem 2.3.10. *The following problem is undecidable:*
Instance: *A TRS $\mathcal{T}$.*
Question: *Is $\mathcal{T}$ confluent?*

As undecidability of confluence is only motivational for this work, but not necessary to understand the rest of this thesis we do not prove it here. The interested reader is however referred to Ohlebusch [19, Chapter 4]. He shows that the contrary to the above theorem would imply Post's correspondence problem (PCP) to be decidable, which stands in contradiction to the well-known fact of PCP's undecidability.

3 A Dual Notion to Transitivity

Duality is a concept that precedes our study of braids as well as our study of self-distributivity and occurs in many fields of computer science and mathematics. However, it may be noticed that we will not find a consistent definition of duality through all the fields. For example, linear programming considers the *dual* problem, projective geometry the *dual* plane, and functional analysis the *dual* space. Nonetheless, all these concepts show a common ground in as much as examining the objects of interest through the principle of duality to induce corresponding properties from the primal to the dual. This chapter introduces duality with respect to transitive relations and is not connected to term rewriting per se.

3.1 Scopic Relations

This section introduces scopic relations via a notion of duality and establishes related properties. Scopic relations were introduced by Guilbaud & Rosenstiehl [20] and the terminology emerged from Melliès [17]. The dual of a function on relations is considered under the following concept.

Definition 3.1.1. The *dual* f^* with respect to a relation R of an n-ary function f on relations is defined by $f^*(U_1, \ldots, U_n) = R - (f(R - U_1, \ldots, R - U_n))$.

Under this definition of duality the dual U^- with respect to a relation R of the transitive closure U^+ of a relation U is given by

$$U^- = R - (R - U)^+.$$

We call U^- the *scopic interior*. Similar to the characterization of a transitive relation as a relation, for which the transitive closure equals the relation itself we call a relation scopic if it equals its scopic interior.

Definition 3.1.2. Let R be a binary relation. $U \subseteq R$ is *scopic* with respect to R if $U^- = U$.

Example 3.1.3. Let $X = \{a, b, c, d\}$ and consider R^+, the transitive closure of the relation R defined by $a\ R\ b\ R\ c\ R\ d$. Then, $U_1 = \{(a, b), (b, c), (a, c)\}$, $U_2 = \{(a, b), (b, c)\}$, $U_3 = \{(a, b)\}$ and $U_4 = \emptyset$ all are scopic with respect to R^+, as $U_i^- = U_i$ for $i \in \{1, 2, 3, 4\}$.

If R of Definition 3.1.2 is clear from the context we may simply say U is scopic. In the upcoming section we will see equivalent characterizations under the assumption that R is transitive, which will be of great importance to us in Section 5.3 and Chapter 6. There, scopic relations with respect to transitive ones turn out as useful tools in proving the corresponding residual identities.

3.2 Scopicness in Company of Transitivity

After defining scopicness we now sharpen the reader's intuition of scopic relations by first showing a necessary condition of scopic relations. This condition will even be proven sufficient in Lemma 3.2.2 if the superrelation is transitive. The remainder of this section generalizes a result from Melliès, as he showed a corresponding statement to Theorem 3.2.6 with respect to a transitive and total relation [17, Theorem 28]. However, as it is shown here the assumption of totality is too strong and it suffices that there exists at most one path between each pair of elements in the transitive reduct. This will be beneficial for us in Chapter 6.

Lemma 3.2.1. *Let R be a binary relation. If $U \subseteq R$ is scopic with respect to R then*

$$a\ R\ b\ R\ c \wedge a\ U\ c \implies a\ U\ b \vee b\ U\ c.$$

Proof. Let $a\ R\ b\ R\ c$ and assume $\neg\,(a\ U\ b)\ \wedge\ \neg\,(b\ U\ c)$, i.e., $a\ (R-U)\ b \wedge b\ (R-U)\ c$. Hence, $a\ (R-U)^+\ c$, which implies $\neg\,(a\ (R-(R-U)^+)\ c)$. Since U is scopic we have $\neg\,(a\ U\ c)$, which proves the claim. □

Intuitively speaking, any element between two elements of a scopic relation stands in some way in relation to either element. We will now give two equivalent characterizations of a relation being scopic under the assumption of the superrelation being transitive. And, as we will consider scopicness only in the presence of transitivity, these characterizations not only help us improve our understanding of a scopic relation but also open up the opportunity to choose the most convenient one in the right situation.

Lemma 3.2.2. *Let R be a binary, transitive relation and $U \subseteq R$. Then the following conditions are equivalent*

1. *U is scopic with respect to R*
2. *$a\ U\ c \implies a\ U\ b \vee b\ U\ c$ for all $a\ R\ b\ R\ c$*
3. *$R-U$ is transitive*

Proof. (1) $\implies$ (2): by Lemma 3.2.1. (2) $\implies$ (3): Let $a\ (R-U)\ b\ (R-U)\ c$, then $\neg\,(a\ U\ b)\ \wedge\ \neg\,(b\ U\ c)$ and $a\ R\ b\ R\ c$, so by the contrapositive of (2) it holds that $\neg\,(a\ U\ c)$. Since R is transitive $a\ R\ c$, hence $a\ (R-U)\ c$. (3) $\implies$ (1): because of transitivity $(R-U)^+ = R-U$, hence $R-(R-U)^+ = R-(R-U) = R \cap U = U$, which proves the claim. □

Hence, for local arguments of a scopic relation such as showing that a certain element is part of the relation, mostly item 2 is the characterization of choice. Proving global properties concerning a scopic relation like the following corollary, it is often convenient to establish corresponding findings in its transitive complement, i.e., item 3 predominates the intuition.

Corollary 3.2.3. *Scopic relations are closed under union.*

Proof. This is an easy consequence of Lemma 3.2.2 (3) and the fact that transitive relations are closed under intersection, using $R - (U \cup V) = (R - U) \cap (R - V)$. □

The constructions of residual systems for braids and self-distributivity rely on the fact that the closure of the union of scopic relations stays scopic. This is the case if the superrelation is transitive. To prove this we introduce a preparatory lemma.

Lemma 3.2.4. *Let R be a transitive relation on X such that for every $u, v \in X$ there exists at most one path from u to v in the transitive reduct of R. Furthermore, let $U \subseteq R$ be scopic with respect to R. Then U^+ is also scopic with respect to R.*

Proof. Assume U^+ is not scopic. Then,

$$\exists a, b, c \in X \text{ with } a\ R\ b\ R\ c \text{ and } a\ U^+\ c \text{ such that } \neg\,(a\ U^+\ b) \text{ and } \neg\,(b\ U^+\ c). \tag{3.1}$$

Out of all a, b, c fulfilling (3.1) choose a triple with the minimal distance of a and c with respect to R. It holds that $\neg\,(a\ U\ c)$, since U is scopic and because of $U \subseteq U^+$ there exists $b' \in X$ different from b with $a\ U^+\ b'\ U^+\ c$. Due to Lemma 2.1.9 it holds that $U^+ \subseteq R$ and by the existence of unique paths in the transitive reduct of R we have $a\ R\ b'\ R\ b\ R\ c$ or $a\ R\ b\ R\ b'\ R\ c$. Without loss of generality assume the latter. Since we chose a and c of minimal distance fulfilling (3.1) it must hold that $b\ U^+\ b'$. However, U^+ is obviously transitive and with $b'\ U^+\ c$ we get the contradiction $b\ U^+\ c$. Hence, U^+ must be scopic with respect to R. □

Note that Lemma 3.2.4 does not hold for arbitrary relations as the following example illustrates.

Example 3.2.5. Let $R = \{(a, b), (a, c), (a, d), (b, c), (d, c)\}$ and $U = \{(a, b), (b, c)\}$. Then U is scopic, since there exists no x with $a\ R\ x\ R\ b$ or with $b\ R\ x\ R\ d$. However, $U^+ = \{(a, b), (b, c), (a, c)\}$, which is not scopic since $a\ R\ d\ R\ c$ and $a\ U^+\ c$ but neither $a\ U^+\ d$ nor $d\ U^+\ c$. See Figure 3.1 and note that two paths from a to c exist, one via b and one via d.

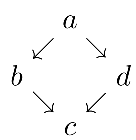


Figure 3.1: The transitive reduct of $R = \{(a, b), (a, c), (a, d), (b, c), (d, c)\}$.

Nonetheless, in our setting of braids and self-distributivity we consider scopic relations in the setting of total orders and prefix orders, respectively. Uniqueness of paths for the former follows, since any totally ordered set is a chain. For the latter one this is ensured as Lemma 2.1.8 shows.

Lastly, we only have to put the collected findings together and prove the main theorem of this chapter generalizing Melliès [17, Theorem 28].

Theorem 3.2.6. *Let R be a transitive relation on X such that for every $u, v \in X$ there exists at most one path from u to v in the transitive reduct of R. Furthermore, let $U, V \subseteq R$ be scopic. Then $(U \cup V)^+$ is scopic as well.*

Proof. By Corollary 3.2.3 the union $U \cup V$ is scopic. Then, using Lemma 3.2.4, the transitive closure $(U \cup V)^+$ is also scopic. □

4 Equivalences of Reductions

The overall goal of this chapter is the introduction of residual systems, which can be seen as skolem functions to the diamond property of many-steps, providing least upper bounds. In other words, the focus lies on the question of what is left to reduce in one step of another co-initial step. Generally, the chapter is a large extract from Terese [23, Chapter 8]. A selection of that chapter is given by van Oostrom and de Vrijer showing four equivalent equivalences of reductions [28]. However, we will not focus on these equivalences but make use of the established findings. Still, the content is introduced so that the motivation behind it becomes comprehensible. The first section introduces proof terms, followed by a section on overlaps of previously introduced proof terms. The third section introduces the concept of tracing, which is later used as model for the diamonds. The last section is finally concerned with residual systems.

4.1 Proof Terms

Before defining proof terms we motivate their introduction by the following example, revealing possible *syntactic accidents* in the relational view of TRS's.

Example 4.1.1. Let $\mathcal{T} = (\Sigma, R)$ be a TRS consisting of the single rule $\rho : f(x) \to x$. Furthermore, let $\to$ be the corresponding relation of the ARS R according to Remark 2.2.4. For a constant a the term $f(f(a))$ relates to exactly one term, namely,

$$f(f(a)) \to f(a).$$

However, substitutions at context $\Box$ and at $f(\Box)$ both witness the above, which is also called a syntactic accident.

The preceding example shows that it is not always evident how we arrived at a term's reduct considering ARS's as rewrite relations. However, since we are interested in reducing the remainder of what is left of one step in another step, it seems to be appropriate to be able to distinguish the two witnesses above. Proof terms provide one way of doing so.

In equational logic we have inference rules for reflexivity, symmetry, transitivity and congruence. Meseguer's rewriting logic is equational logic without symmetry [18]. Proof terms capture this idea and pose term representations for reduction sequences of an associated TRS by means of rewriting logic instead of equational logic, i.e., there exists no proof term corresponding to an inference rule for symmetry. To simplify the theory even further we also do not employ a proof term corresponding to the inference rule of reflexivity, as is done in Terese and the corresponding article by van Oostrom & de Vrijer [23, 28]. We justify this after we have given a formal definition of proof terms.

Definition 4.1.2. Let $\mathcal{T} = (\Sigma, R)$ be a TRS. The disjoint union of Σ, R and a binary composition symbol $\{\cdot\}$ is called the *proof term signature* of $\mathcal{T}$, where each rule ρ in R, also denoted by ρ, is associated with the number of free variables in the left-hand side as its arity. In case $\rho : \ell \to r$ is a rule with n free variables in ℓ we denote by $\ell(s_1, \ldots, s_n)$ and $r(s_1, \ldots, s_n)$ the terms obtained by substituting s_i in ℓ and r for the ith variable in ρ, respectively, assuming the variables are sequenced in an arbitrary but fixed order.

Hence, the proof term signature supplements the signature of a TRS by its rule symbols and a composition symbol. On the basis of that signature an underlying ARS is defined.

Definition 4.1.3. Let $\mathcal{T} = (\Sigma, R)$ be a TRS. The *underlying* abstract rewrite system $\geq_{\mathcal{T}}$ is defined as follows:

- The objects are terms over Σ.
- The steps are a subset of the terms over the proof term signature of $\mathcal{T}$. They are inductively defined by the following inference system:

$$\frac{\phi_1 : s_1 \geq_{\mathcal{T}} t_1 \qquad \ldots \qquad \phi_n : s_n \geq_{\mathcal{T}} t_n}{f(\phi_1, \ldots, \phi_n) : f(s_1, \ldots, s_n) \geq_{\mathcal{T}} f(t_1, \ldots, t_n)} \; (\textsc{Rep})$$

$$\frac{\phi_1 : s_1 \geq_{\mathcal{T}} t_1 \qquad \ldots \qquad \phi_n : s_n \geq_{\mathcal{T}} t_n}{\rho(\phi_1, \ldots, \phi_n) : \ell(s_1, \ldots, s_n) \geq_{\mathcal{T}} r(t_1, \ldots, t_n)} \; (\textsc{Rule})$$

$$\frac{\phi : s \geq_{\mathcal{T}} t \qquad \psi : t \geq_{\mathcal{T}} u}{(\phi \cdot \psi) : s \geq_{\mathcal{T}} u} \; (\textsc{Transitivity})$$

  The above inference system also defines the src- and tgt-functions.

Remark 4.1.4. (Rep) is an abbreviation for Replacement. If $\mathcal{T}$ is clear from the context we may write $\geq$ instead of $\geq_{\mathcal{T}}$.

By the underlying ARS $\geq_{\mathcal{T}}$ of a TRS $\mathcal{T}$ we defined term representations of reduction sequences or, as they are also called, of proofs, which finally define proof terms. Hence, proof terms are proof of reachability, i.e., if $\phi : s \geq_{\mathcal{T}} t$ the proof term ϕ proves that t is reachable from s using the rules replacement, rule, and transitivity.

Definition 4.1.5. Let $\mathcal{T} = (\Sigma, R)$ be a TRS. A *proof term* (or just *proof*) is a step of the underlying ARS $\geq_{\mathcal{T}}$.

Remark 4.1.6. As mentioned in the introduction to this section no proof term corresponding to the inference rule of reflexivity is defined. It might seem unavoidable to have an inference rule à la

$$\frac{}{1_s : s \geq_{\mathcal{T}} s} \; (\textsc{Reflexivity})$$

for rewriting logic. However, as stated by van Oostrom & de Vrijer, constants and variables behave in like manner with respect to permutation equivalence, which they show equivalent to projection equivalence [28]. And since we are interested in proof terms with respect to residual systems defining a projection equivalence, we can safely assume proof terms to be ground. Furthermore, the replacement-rule applied to constants provides us with a way to derive $s : s \geq_{\mathcal{T}} s$ for any ground term s. Hence, a rule for reflexivity would be redundant for our purposes.

The next theorem shows that proof terms indeed represent what we intended them to represent.

Theorem 4.1.7. *Let $\mathcal{T} = (\Sigma, R)$ be a TRS. Then, $\rightarrow^*_{\mathcal{T}} = \geq_{\mathcal{T}}$.*

Proof. Given an inference step of $\rightarrow^*$, we can naturally find a proof term representation. 1_a translates to a, a $\mathcal{T}$-step translates to 'itself' and composition translates to composition. Vice versa, by an easy induction on the proof terms a characterization in $\rightarrow^*$ is shown. □

Note that in the proof above we implicitly handled $x \rightarrow^* x$ for x a variable as mentioned in Remark 4.1.6. With Theorem 4.1.7 in mind we now can suitably restrict the underlying ARS and obtain equivalents to multi-step, parallel step and single-step rewriting.

Definition 4.1.8. Let $\multimap_{\mathcal{T}} := \langle A, \Phi_0, \mathrm{src}_0, \mathrm{tgt}_0 \rangle$, $\dashrightarrow\!\!\!\!\!\!\parallel\;\; := \langle A, \Phi_1, \mathrm{src}_1, \mathrm{tgt}_1 \rangle$ and $\rightarrow_{\mathcal{T}} := \langle A, \Phi_2, \mathrm{src}_2, \mathrm{tgt}_2 \rangle$ be defined as the sub-abstract-rewrite-systems of $\geq_{\mathcal{T}} := \langle A, \Phi, \mathrm{src}, \mathrm{tgt} \rangle$, such that

- $\Phi_0 \subseteq \Phi$ is the set defined by the proof terms consisting only of function and rule symbols over the proof term signature of $\mathcal{T}$,
- $\Phi_1 \subseteq \Phi_0$ is the set defined by the proof terms consisting furthermore of no nested rule symbols,
- $\Phi_2 \subseteq \Phi_1$ is the set defined by the proof terms consisting of exactly one rule symbol,

and $\mathrm{src}_i, \mathrm{tgt}_i$ the restriction of Φ_i for $i \in \{0, 1, 2\}$. Steps in $\multimap_{\mathcal{T}}$ are called *multi*-steps of $\mathcal{T}$, steps in $\dashrightarrow\!\!\!\!\!\!\parallel_{\mathcal{T}}$ are called *parallel* steps of $\mathcal{T}$ and steps in $\rightarrow_{\mathcal{T}}$ are called *(single-)* steps of $\mathcal{T}$. If $\mathcal{T}$ is clear from the context we may omit the subscript and write $\multimap$, $\dashrightarrow\!\!\!\!\!\!\parallel$ or $\rightarrow$ instead.

Remark 4.1.9. The inference steps as, e.g., in [23, Definitions 4.7.1, 4.7.3, 4.7.11] each correspond to an inference step for proof terms, vice versa, by an easy induction on the respectively defined subsets of the proof terms a relational characterization can be derived. For this reason above defined notions of single-step, parallel step and multi-step indeed coincide with the respective concepts of relational rewriting.

Example 4.1.10. Consider the TRS $\mathcal{T}$ defined by $\{\rho : f(f(x)) \rightarrow x, \varsigma : g(f(x), y) \rightarrow g(x, f(y))\}$. The proof term $\varsigma(a, \rho(b)) : g(f(a), f(f(b))) \multimap_{\mathcal{T}} g(a, f(b))$ defines a multi-step, $g(\rho(a), \rho(b)) : g(f(f(a)), f(f(b))) \dashrightarrow\!\!\!\!\!\!\parallel_{\mathcal{T}} g(a, b)$ a parallel-step and $g(\rho(a), b) : g(f(f(a)), b) \rightarrow_{\mathcal{T}} g(a, b)$ a single-step.

The next corollary is a simple conclusion from Definition 4.1.8 and confirms the understanding the reader might already have from the relational point of view.

Corollary 4.1.11. $\rightarrow_{\mathcal{T}} \subseteq \mathrel{-\!\!\!\parallel\!\!\!\rightarrow}_{\mathcal{T}} \subseteq \mathrel{-\!\!\circ\!\!\rightarrow}_{\mathcal{T}} \subseteq \geq_{\mathcal{T}}$.

Coming back to Example 4.1.1 we now have a simple way of distinguishing each witness, which is illustrated below.

Example 4.1.12. Let $\mathcal{T}$ be the TRS from Example 4.1.1. The two single-step derivations

$$\dfrac{\dfrac{\dfrac{}{a : a \geq_{\mathcal{T}} a}\ (\textsc{Rep})}{f(a) : f(a) \geq_{\mathcal{T}} f(a)}\ (\textsc{Rep})}{\rho(f(a)) : f(f(a)) \geq_{\mathcal{T}} f(a)}\ (\textsc{Rule}) \qquad \dfrac{\dfrac{\dfrac{}{a : a \geq_{\mathcal{T}} a}\ (\textsc{Rep})}{\rho(a) : f(a) \geq_{\mathcal{T}} a}\ (\textsc{Rule})}{f(\rho(a)) : f(f(a)) \geq_{\mathcal{T}} f(a)}\ (\textsc{Rep})$$

are both witnesses to $f(f(a)) \rightarrow f(a)$.

4.2 Overlaps

In the previous section we saw proof terms as an appropriate representation of reductions. Now, we will focus on the interaction of two co-initial proof terms and give a definition of orthogonality. We consider orthogonality as a property between two steps, rather than as a property of rewrite systems. We further show that orthogonal steps can equivalently be described as having no overlap. The study of orthogonal systems is motivated by the fact that, as we will see later, theses systems ensure confluence. Furthermore, constructing a residual system for orthogonal TRS's provide first and valuable insights for our overall goal of a construction of a residual system for self-distributivity. Hence, they will accompany us throughout this thesis and serve as an initial example.

In the following section we will use contexts in combination with proof terms. So, from here on we supplement the proof term signature with the constant $\Box$ implicitly when needed, and begin this section by defining overlaps.

Definition 4.2.1. Let $\mathcal{T} = (\Sigma, R)$ be a TRS.

- s is a *ρ-redex*, if there exists a substitution σ such that $s = \mathrm{src}(\rho(x_1^\sigma, \ldots, x_n^\sigma))$ for $\rho \in R$.
- The *ρ-pattern* of a rule $\rho : l \rightarrow r \in R$ is defined as the proof term $\rho(\Box, \ldots, \Box)$ for $\rho \in R$.
- The *pattern* of a single-step $\phi : s \rightarrow_{\mathcal{T}} t$ is a proof term resulting from replacing the sub-term with $\rho \in R$ as head symbol by its corresponding ρ-pattern in ϕ.
- A function symbol occurrence $\langle f \mid C[\ ]\rangle$ in s is *rule-based* with respect to a single-step $\phi : s \rightarrow_{\mathcal{T}} t$, if it is not a function symbol occurrence in ϕ and the source of the pattern of ϕ is not a prefix of $C[\ ]$. In that case, we also call $\langle f \mid C[\ ]\rangle$ *rule-based* in ϕ.
- Two co-initial single-steps ϕ, ψ *overlap*, if there exists $\langle f \mid C[\ ]\rangle$, which is a rule-based function symbol occurrence in ϕ and ψ. The overlap is *trivial*, if $\phi = \psi$.

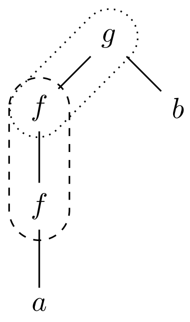


Figure 4.1: Visualizing overlap of two co-initial single-steps $\phi = g(\rho(a), b)$ and $\psi = \varsigma(f(a), b)$ with $\rho : f(f(x)) \to x$ (dashed) and $\varsigma : g(f(x), y) \to g(x, f(y))$ (dotted) at function symbol occurrence $\langle f \mid g(\Box, b)\rangle$.

- Two rules $\rho, \varsigma \in R$ *overlap*, if there exist two distinct co-initial single-steps $\phi : s \to_{\mathcal{T}} t_1, \psi : s \to_{\mathcal{T}} t_2$, such that ϕ and ψ overlap, due to ρ in ϕ and due to a ς in ψ.

- $\mathcal{T}$ is called *overlapping* or *ambiguous*, if for any pair $\rho, \varsigma \in R$ of rules ρ and ς do not overlap. Otherwise $\mathcal{T}$ is called *non-overlapping* or *non-ambiguous*.

Remark 4.2.2. Note, that an overlap of two single-steps is solely determined by their sources.

Hence, two co-initial single-steps overlap, if they share a function symbol occurrence in their source, which is rule-based in both steps. The condition on the pattern of ϕ not being a prefix of $C[\ ]$ defining rule-based, especially excludes an 'overlap' at a rule's variable position.

Example 4.2.3. Let $(\Sigma, \to)$ be a TRS consisting of the rules $\rho : f(f(x)) \to x$ and $\varsigma : g(f(x), y) \to g(x, f(y))$. The two steps $\phi = g(\rho(a), b) : g(f(f(a)), b) \to g(a, b)$ and $\psi = \varsigma(f(a), b) : g(f(f(a)), b) \to g(f(a), f(b))$ are then co-initial. There exist five function symbol occurrences in $g(f(f(a)), b)$, namely, $\langle g \mid \Box\rangle$, $\langle f \mid g(\Box, b)\rangle$, $\langle f \mid g(f(\Box), b)\rangle$, $\langle a \mid g(f(f(\Box)), b)\rangle$ and $\langle b \mid g(f(f(a)), \Box)\rangle$, where the first is only rule-based in ψ, the second is rule-based in ϕ as well as in ψ and, where the third is only rule-based in ϕ. The latter two function symbol occurrences are neither rule-based in ϕ nor in ψ. Hence, ϕ, ψ overlap due to the second function symbol occurrence and so do ρ, ς (see Figure 4.1).

Now, two co-initial single-steps are defined as orthogonal, if we can join them into one proof term, without composition, i.e., if they do not overlap. We distinguish two types of orthogonality. First, horizontal orthogonality denoting the rule symbols being in parallel sub-terms and vertical orthogonality denoting the rule symbols being above each other.

Definition 4.2.4. Let $\phi : s \to_{\mathcal{T}} t_1, \psi : s \to_{\mathcal{T}} t_2$ be distinct, co-initial single-steps in a left-linear TRS $\mathcal{T} = (\Sigma, R)$, such that $\phi = C[\rho(x_1^\sigma, \dots, x_n^\sigma)]$, $\psi = D[\varsigma(x_1^\tau, \dots, x_m^\tau)]$ with $\rho, \varsigma \in R$ and σ, τ substitutions. If neither $C[\ ]$ is a prefix of $D[\ ]$ nor vice versa, ϕ and ψ are *horizontally* orthogonal. If $C[\ ]$ is a prefix of $D[\ ]$ and there exists no function symbol occurrence in s, which is a rule-based function symbol occurrence of ϕ and ψ, the steps are *vertically* orthogonal. The steps ϕ, ψ are called *orthogonal* if they are either vertically or horizontally orthogonal and we write $\phi \perp \psi$.

Next, we show that orthogonality of two co-initial single-steps is equivalent to the absence of overlaps. It may be noted that orthogonality of steps is defined for left-linear TRS's only. Hence, assuming two steps to be orthogonal implies them to be left-linear.

Theorem 4.2.5. *Let $\phi : s \to_{\mathcal{T}} t_1$ and $\psi : s \to_{\mathcal{T}} t_2$ be co-initial single-steps. ϕ and ψ are horizontally or vertically orthogonal, if and only if they do not overlap.*

Proof. (If-direction) Let ϕ, ψ be horizontally orthogonal. Then there exist contexts $C[\ ], D[\ ]$ and substitutions σ, τ with $\phi = C[\rho(x_1^\sigma, \ldots, x_n^\sigma)]$, $\psi = D[\varsigma(x_1^\tau, \ldots, x_m^\tau)]$, such that neither $D[\ ]$ is a prefix of $C[\ ]$ nor vice versa. Hence, rule-based function symbol occurrences in ϕ will not coincide with rule-based function symbol occurrences in ψ.

Let ϕ, ψ be vertically orthogonal. The claim is a direct consequence of the definition of vertical orthogonality, which excludes overlaps.

(Only-if direction) We show the equivalent statement, that if ϕ and ψ are neither horizontally nor vertically orthogonal they overlap. Let $\phi = C[\rho(x_1^\sigma, \ldots, x_n^\sigma)]$, $\psi = D[\varsigma(x_1^\tau, \ldots, x_m^\tau)]$ with σ, τ substitutions for the contexts $C[\ ], D[\ ]$. If ϕ and ψ are not horizontally orthogonal one of the contexts is a prefix of the other. Without loss of generality assume $C[\ ]$ to be a prefix of $D[\ ]$. Since ϕ and ψ are not vertically orthogonal, there exists either no function symbol occurrence in s at all, or there exists a function symbol occurrence, which is a rule based function symbol occurrence in ϕ and ψ. The former case implies s to be a single variable, which is impossible due to the definition of TRS. Hence, ϕ and ψ overlap. ☐

On the basis of orthogonal steps we define orthogonal term rewriting systems, such that no pair of rules overlap.

Definition 4.2.6. A TRS $\mathcal{T} = (\Sigma, R)$ is orthogonal if $\mathcal{T}$ is left-linear and for all pairs $\rho, \varsigma \in R$ it holds that ρ, ς do not overlap.

Remark 4.2.7. Note, that in Definition 4.2.6 we do not exclude overlaps of the same rule, but we only exclude trivial overlaps as steps have to be distinct in Definition 4.2.1.

Justifying the naming of an orthogonal TRS, we show that, as one would expect, steps in such a system are indeed orthogonal.

Corollary 4.2.8. *Two distinct co-initial single-steps in an orthogonal TRS are orthogonal.*

Proof. Direct consequence from the definition of orthogonal TRS and rule overlap. ☐

We extend the definition of orthogonality to parallel steps and multi-steps by thinking of them as a collection of single-steps. If all single-steps are mutually orthogonal between the two collections we consider the collections orthogonal. Below this idea is formalized.

Definition 4.2.9. Let ϕ, ψ be co-initial multi-steps.

- We define $\phi' \Subset \phi$ if ϕ' is obtained by replacing all but one rule symbol by their left-hand side, i.e., ϕ rewrites to ϕ' by rewrite rules $\rho(x_1, \ldots, x_n) \to \ell(x_1, \ldots, x_n)$ for $\rho : \ell \to r \in R$.
- A function symbol occurrence o is *rule-based* for a multi-step $\phi : s \multimap_{\mathcal{T}} t$ if there exists a single-step $\phi' \Subset \phi$ such that o is a rule-based function symbol occurrence in ϕ'.
- Two distinct multi-steps ϕ, ψ are *orthogonal* if for all distinct pairs $\phi' \Subset \phi, \psi' \Subset \psi$ the single-steps ϕ', ψ' are orthogonal.
- ϕ, ψ *overlap* if there exist $\phi' \Subset \phi, \psi' \Subset \psi$ such that ϕ', ψ' overlap. We call the overlap *trivial*, if $\phi = \psi$.

As first examples for residual systems we will see systems for multi-steps and parallel-steps, respectively. For multi-steps a similar equivalence holds, as it does for single-steps.

Corollary 4.2.10. *Let ϕ, ψ be co-initial multi-steps. If ϕ, ψ are orthogonal they do not overlap. If ϕ, ψ are not orthogonal they overlap.*

Proof. Direct consequence of Theorem 4.2.5. □

As parallel-steps are a sub-ARS of multi-steps the same result obviously holds for parallel-steps as well.

We end this section addressing the necessary condition of left-linearity for orthogonal systems. In general, orthogonality implies confluence, which will be proven later in the context of residual systems, however, non-ambiguity alone is not enough as Klop showed [14, Chapter 3]. The following summarizes Klop's counter example.

Example 4.2.11. Let $\mathcal{T}$ be a TRS, consisting of the rewrite rules $\{\rho : g(x, x) \to b, \varsigma : f(x) \to g(x, f(x)), \vartheta : a \to f(a)\}$. Due to ρ the system is not left-linear. Moreover, it is non-ambiguous, as each left-hand side consists of a single function symbol and no pair of left-hand sides contain the same symbol, i.e., no two co-initial single-steps can share a function symbol occurrence.

To see that $\mathcal{T}$ is not confluent, note that there exist co-initial reductions $\phi : a \twoheadrightarrow b$ and $\psi : a \twoheadrightarrow f(b)$ of $\to$. However, b is a normal form and the only reductions of $\to$ having $f(b)$ as source have $g(b, g(b, g(\ldots, g(b, f(b)) \ldots)))$ as target. As a consequence the system is not confluent.

4.3 Tracing

After we saw how to determine an overlap between proof terms in the last section we now introduce tracing, which provides a way to follow the behaviour of sub-terms along reductions. This is done by relating positions in the source to positions in the target of rules and then naturally extend the procedure to proof terms by means of an algebra. In this way properties are *traced* from the source through to the target of a reduction. This is particularly useful for us regarding associativity, since we will see that proof terms on both paths of a diamond induce the same relation. For this reason each sub-term in the source behaves equally no matter what path we take. Obviously this also applies to redex-patterns being the key to its residual system. We will transfer this method from associativity to self-distributivity and apply it similarly.

Generally, Σ-algebras provide a semantic interpretation of terms. Concerning associativity and self-distributivity, we are going to consider the Σ-algebra, where Σ is the proof term signature of the respective TRS $\mathcal{T}$, having relations between positions as carrier. We call this algebra hereafter the *proof term algebra* $\mathfrak{A}$ of the TRS $\mathcal{T}$. Before specifying the interpretation of proof terms, we are going to introduce rule tracings, on which the interpretations will depend.

Definition 4.3.1. Let $\mathcal{T} = (\Sigma, R)$ be a TRS. A *rule tracing* of $\rho : \ell \to r \in R$ is a relation $[\rho\rangle \subseteq \mathcal{P}os(\ell) \times \mathcal{P}os(r)$, such that ϵ relates to one or more non-variable positions in r, other non-variable positions in ℓ relate to zero or more non-variable positions in r and variables relate to themselves, i.e. $p\ [\rho\rangle\ q$, if $\ell|_p = x = r|_q$ for variable x. The case, where r is merely a single variable is an exception allowing non-variable positions in ℓ to relate to the variable position ϵ in r, especially $(\epsilon, \epsilon) \in [\rho\rangle$.

Hence, by above definition we trace the positions of the left-hand sides to the right-hand sides of a rule. Positions of variables in the left-hand side relate to all positions of the same variable of the right-hand side. Non-variable positions of the left-hand side may but don't need to relate to non-variable positions of the right-hand side, except the case where r is exactly one variable, where we allow non-variable positions to relate to the single variable. Furthermore, the position of the head symbol of the left-hand side always relates to a position of the right-hand side. We exemplary illustrate this at the TRS we already saw in Section 4.2.

Example 4.3.2. Consider the TRS of Example 4.2.3, consisting of the rules $\rho : f(f(x)) \to x$ and $\varsigma : g(f(x), y) \to g(x, f(y))$. Then, $[\rho\rangle = \{(\epsilon, \epsilon), (0, \epsilon), (00, \epsilon)\}$ and $[\varsigma\rangle = \{(\epsilon, \epsilon), (0, 1), (00, 0), (1, 10)\}$ define corresponding rule tracings.

The relation $\{(00, \epsilon)\}$ does not represent a rule tracing for ρ as the head symbol of the left-hand side leaves no trace in the right-hand side. The relation $\{(\epsilon, 1), (0, 0), (00, 0), (1, 10)\}$ does not represent a rule tracing for ς as the non-variable position 0 in the left-hand side relates to the variable position 0 in the right-hand side.

To define the interpretation of a proof term algebra we adhere to the following notation concerning functions of relations.

Notation 4.3.3. Let $T = (\Sigma, R)$ be a TRS with a given rule tracing $[\rho\rangle$ for each $\rho \in R$ and let $R_1, \ldots, R_n$ be relations on positions.

- For $f \in \Sigma$ the expression $f(R_1, \ldots, R_n)$ is notation for the relation, which relates ϵ to ϵ and $i \cdot p$ to $i \cdot q$ if $p\ R_i\ q$.

- For $\rho \in R$ with $\rho : \ell \to r$ the expression $\rho(R_1, \dots R_n)$ is notation for the relation, which relates p to q if $p\ [\rho\rangle\ q$ as well as $p \cdot p'$ to $q \cdot q'$ if p is a variable position at x_i in ℓ with $p\ [\rho\rangle\ q$ and $p'\ R_i\ q'$.

Now, a trace relation of a proof term ϕ is an interpretation in the corresponding proof term algebra defined by a given set of rule tracings.

Definition 4.3.4. Let $\mathcal{T} = (\Sigma, R)$ be a TRS with a given set of rule tracings $P = \{[\rho\rangle \mid \rho \in R\}$ (by P we denote the capital ρ). The interpretation of $\phi : s \geq_{\mathcal{T}} t$ in the proof term algebra of $\mathcal{T}$ is inductively defined as a relation $[[\phi\rangle\rangle_P \subseteq \mathcal{P}os(s) \times \mathcal{P}os(t)$ by

$$[[\phi\rangle\rangle_P := \begin{cases} f([[\phi_1\rangle\rangle_P, \dots, [[\phi_n\rangle\rangle_P) & \text{if } \phi = f(\phi_1, \dots, \phi_n) \text{ with } f \in \Sigma \\ \rho([[\phi_1\rangle\rangle_P, \dots, [[\phi_n\rangle\rangle_P) & \text{if } \phi = \rho(\phi_1, \dots, \phi_n) \text{ with } \rho \in R \\ [[\phi_1\rangle\rangle_P \cdot [[\phi_2\rangle\rangle_P & \text{if } \phi = \phi_1 \cdot \phi_2 \end{cases}$$

under Notation 4.3.3. The relation $[[\phi\rangle\rangle_P$ is called the *trace relation* of ϕ. If P is clear from the context we write $[[\phi\rangle\rangle$ instead of $[[\phi\rangle\rangle_P$.

So, proof terms are interpreted as relations according to a given set of rule tracings and proof term composition is interpreted as relation composition. As a unit proof term relates its source to itself we interpret it as the identity relation. Intuitively, the trace relation can be seen as a natural extension from the rule tracings to proof terms. Next, we carry this extension out and derive a trace relation of the proof terms from the previous section's example.

Example 4.3.5. Consider the TRS and the corresponding set of rule tracings P from Example 4.3.2. The trace relations of the proof terms from Example 4.2.3, i.e., $\phi = g(\rho(a), b)$ and $\psi = \varsigma(f(a), b)$, are then given by $[[\phi\rangle\rangle_P = \{(\epsilon, \epsilon), (0, \epsilon), (00, \epsilon), (000, \epsilon), (1, 1)\}$, and $[[\psi\rangle\rangle_P = \{(\epsilon, \epsilon), (0, 1), (00, 0), (000, 00), (1, 10)\}$, respectively.

For the rewrite system of associativity in Section 5.2 and of self-distributivity in Section 6.4, we will show that the established trace relations of the left and right side of a diamond are equal. This result ensures that tracing a redex-pattern along either side results in the same pattern, and, as we will furthermore define steps via redex-patterns, this gives us sort of an associative property.

4.4 Residual Systems

In preceding sections proof terms were introduced, their overlaps discussed and orthogonal systems defined. Afterwards, proof term algebras were presented. Next, residual systems are established providing confluence.

Comparing the confluence property (Definition 2.2.9) with the diamond property (Definition 2.2.5) it becomes apparent that confluence is nothing more than the diamond property for reductions. Eliminating existential quantifiers of the diamond property results for the skolem function f, g in the following: For all $\phi : s \to t_1, \psi : s \to t_2$ it holds that $f(\phi, \psi) : t_1 \to t, g(\phi, \psi) : t_2 \to t$. By symmetry and the axiom of choice we can assume $f(\phi, \psi) = g(\psi, \phi)$. Hence, *For all* $\phi : s \to t_1, \psi : s \to t_2$ *it holds that* $g(\psi, \phi) : t_1 \to t, g(\phi, \psi) : t_2 \to t$.

A witness to the function g is called a residuation and is denoted by /. If the residuation fulfils certain axioms for an ARS together with a unit the triple defines what is called in Terese a residual system [23, Section 8.7]. As for many rewrite systems the diamond property does not hold we will enrich the system in a *minimal* way when possible by the compositions of steps necessary for the diamond property to hold, which is called *faceting* by van Oostrom [26], hence, we consider reductions. To form the intuition on the implications of the axioms for a residuation in a residual system consider the next exemplary illustration.

When we think of a reduction as a collection of tasks, we can quasi-order co-initial steps by considering, whether or not there are tasks left in a collection after we have done all tasks of another collection. As an example, let the tasks be to gather groceries, i.e., the collection of tasks are shopping lists. The mini-market you are at has the items 1 to 10. Shopping list A consists of the items 3,4,5 and shopping list B comprises the items 2,4,6. The two lists are incomparable, as doing A first leaves still 2 and 6 to collect in B. Doing B first leaves 3 and 5 to collect in A. Now confluence is the property that a list incorporating the tasks of A and B can always be found. One easy way would be to follow a list C collecting all items 1 to 10 of the mini-market, as there would no tasks of neither list be left. Hence, both A and B are smaller than C. Residual systems provide us with the list consisting exactly of the items 2 to 6, i.e., a list which is an upper bound to both but also smaller than any other upper bound. Differently said, no tasks are left to do but also no superfluous work has been done.

Not surprisingly this intuition is overly simplified and rather fits orthogonal systems as tasks are independent of each other, i.e., have no overlap. However, we could face the situation that, e.g., doing 2 changes 3 to 7 or other dependencies such as 3 and 2 together also require 1, which will be the case in Chapter 5 and 6. Formalizing the intuition above we first define residuation.

Definition 4.4.1. Let $\to := \langle A, \Phi, \mathrm{src}, \mathrm{tgt}\rangle$ be an ARS. Furthermore, let $D \subseteq \Phi \times \Phi$ denote the set of co-initial steps in Φ and let $/ : D \to \Phi$ be a function from co-initial steps to steps. If $\mathrm{tgt}(\phi) = \mathrm{src}(/(\psi, \phi))$ and $\mathrm{tgt}(/(\phi, \psi)) = \mathrm{tgt}(/(\psi, \phi))$ the function / is called a residuation for $\to$. We may sometimes refer to a residuation as a residual function and we may write / in infix notation, i.e., ψ/ϕ for $/(\psi, \phi)$.

Then, a residual system is a triple consisting of an ARS, a unit and a residuation fulfilling certain axioms.

Definition 4.4.2. A residual system is a triple $\langle \to, 1, / \rangle$, that satisfies the residual identities:

$$(\phi/\psi)/(\chi/\psi) \approx (\phi/\chi)/(\psi/\chi) \tag{R1}$$

$$\phi/\phi \approx 1 \tag{R2}$$

$$\phi/1 \approx \phi \tag{R3}$$

$$1/\phi \approx 1 \tag{R4}$$

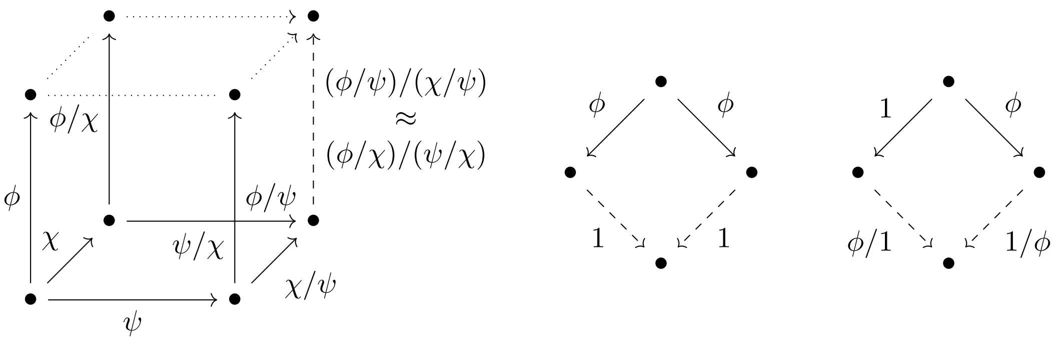


Figure 4.2: Visualization of the residual identities R1–R4.

where / is a residuation for the ARS $\to = \langle A, \Phi, \mathrm{src}, \mathrm{tgt}\rangle$ with the unit 1 and $\phi, \psi, \chi \in \Phi$.

Remark 4.4.3. We pronounce ϕ/ψ as ϕ *after* ψ. R1 is also referred to as the *cube* identity. R2–R4 are also referred to as the *unit* identities (see Figure 4.2).

The cube identity expresses that performing the step ϕ after either path of the bottom face of the cube in Figure 4.2 results in the same step. As an intuition for the unit identities we can call the unit 1 a loop. R2 then reads as *a step after itself is a loop*, R3 as *a step after a loop is the step again* and R4 as *a loop after a step is again a loop*.

The first examples of residual systems are given by parallel step and multi-step rewriting for orthogonal systems. According to the intuition of the entry example to this section tasks correspond to pairwise orthogonal single-steps collected in parallel steps and multi-steps, respectively. We first define a corresponding residuation.

Lemma 4.4.4. *The function / defined by*

$$\phi/\psi := \begin{cases} f(\phi_1/\psi_1, \dots, \phi_n/\psi_n) & \text{if } \phi = f(\phi_1, \dots, \phi_n), \psi = f(\psi_1, \dots, \psi_n) \\ \rho(\phi_1/\psi_1, \dots, \phi_n/\psi_n) & \text{if } \phi = \rho(\phi_1, \dots, \phi_n), \psi = \ell(\psi_1, \dots, \psi_n), \rho : \ell \to r \\ r(\phi_1/\psi_1, \dots, \phi_n/\psi_n) & \text{if } \phi = \ell(\phi_1, \dots, \phi_n),\ \psi = \rho(\psi_1, \dots, \psi_n), \rho : \ell \to r \\ r(\phi_1/\psi_1, \dots, \phi_n/\psi_n) & \text{if } \phi = \rho(\phi_1, \dots, \phi_n), \psi = \rho(\psi_1, \dots, \psi_n), \rho : \ell \to r \end{cases}$$

is a residuation for $\mathrel{-\!\!\|\!\!\rightarrow}_{\mathcal{T}}$ *and* $\mathrel{-\!\!\circ\!\!\rightarrow}_{\mathcal{T}}$ *with* $\phi \perp \psi$.

Proof. First, we show that / is well-defined. Consider the function symbol occurrence $\langle f \mid \square\rangle$ in s and consider two co-initial multi-steps $\phi : s \mathrel{-\!\!\circ\!\!\rightarrow}_{\mathcal{T}} t_1, \psi : s \mathrel{-\!\!\circ\!\!\rightarrow}_{\mathcal{T}} t_2$. We have three cases to distinguish:

(a) $\langle f \mid \square\rangle$ is not a rule-based function symbol occurrence in either ϕ or ψ, hence f is a function symbol of ϕ and ψ and ϕ_i, ψ_i are co-initial again, since ϕ and ψ are.

(b) $\langle f \mid \square\rangle$ is a rule-based function symbol occurrence in either ϕ or ψ. Assume f is the head symbol of the left-hand side of ρ and without loss of generality $\langle f \mid \square\rangle$ is rule-based in ϕ, i.e. $\phi = \rho(\phi_1, \dots, \phi_n)$ and since ϕ, ψ are co-initial it follows that $\psi = \ell(\psi_1, \dots, \psi_n)$ and that ϕ_i, ψ_i are co-initial again.

	ϕ	ψ	χ
1	$f(\phi_1,\ldots,\phi_m)$	$f(\psi_1,\ldots,\psi_m)$	$f(\chi_1,\ldots,\chi_m)$
2	$\rho(\phi_1,\ldots,\phi_n)$	$\ell(\psi_1,\ldots,\psi_n)$	$\ell(\chi_1,\ldots,\chi_n)$
3	$\ell(\phi_1,\ldots,\phi_n)$	$\rho(\psi_1,\ldots,\psi_n)$	$\ell(\chi_1,\ldots,\chi_n)$
4	$\rho(\phi_1,\ldots,\phi_n)$	$\rho(\psi_1,\ldots,\psi_n)$	$\ell(\chi_1,\ldots,\chi_n)$
5	$\ell(\phi_1,\ldots,\phi_n)$	$\ell(\psi_1,\ldots,\psi_n)$	$\rho(\chi_1,\ldots,\chi_n)$
6	$\rho(\phi_1,\ldots,\phi_n)$	$\ell(\psi_1,\ldots,\psi_n)$	$\rho(\chi_1,\ldots,\chi_n)$
7	$\ell(\phi_1,\ldots,\phi_n)$	$\rho(\psi_1,\ldots,\psi_n)$	$\rho(\chi_1,\ldots,\chi_n)$
8	$\rho(\phi_1,\ldots,\phi_n)$	$\rho(\psi_1,\ldots,\psi_n)$	$\rho(\chi_1,\ldots,\chi_n)$

Table 4.1: Comparing the possible proof term structures of three co-initial multi-steps ϕ, ψ and χ with $\mathcal{T} = (\Sigma, R)$ orthogonal and $\rho : \ell \to r \in R$.

(c) $\langle f \mid \Box \rangle$ is a rule-based function symbol occurrence in both ϕ and ψ. Since $\phi \perp \psi$ the single-steps $\phi' \in \phi$ and $\psi' \in \psi$ where the rule-based function symbol occurrence originate from (see Definition 4.2.9) must coincide, hence, $\phi = \rho(\phi_1, \ldots, \phi_n)$ and $\psi = \rho(\psi_1, \ldots, \psi_n)$. In that case ϕ_i, ψ_i are obviously co-initial.

Since the inductive structure of / is defined on proof terms the case in (b) and (c) where f is not a head symbol in s does not occur. It follows that for any pair of co-initial multi-steps exactly one clause defining / applies, hence / is total on co-initial, orthogonal multi-steps and, thus, total on orthogonal parallel steps as well.

By induction on the clauses of / it follows that ϕ/ψ is a multi-step again for ϕ, ψ multi-steps and a parallel step for ϕ, ψ parallel steps.

By another induction on the clauses of / it is easy to prove that $\mathrm{tgt}(\phi) = \mathrm{src}(\psi/\phi)$ and $\mathrm{tgt}(\psi/\phi) = \mathrm{tgt}(\phi/\psi)$ holds. □

By induction we show that parallel steps and multi-steps also constitute residual systems for orthogonal rewriting.

Lemma 4.4.5. *Let $\mathcal{T}$ be an orthogonal TRS. $\langle \twoheadrightarrow\!\!\!\!\!\!\!+\;\;_{\mathcal{T}}, 1, / \rangle$ as well as $\langle \multimap_{\mathcal{T}}, 1, / \rangle$ both constitute a residual system for the residuation / defined in Lemma 4.4.4.*

Proof. The claim is shown by structural induction on proof terms. To do so and since $\mathcal{T}$ is orthogonal, we have to distinguish 8 different cases to show R1, see Table 4.1. Note that $\ell(\phi_1, \ldots, \phi_n)/\ell(\psi_1, \ldots, \psi_n) = \ell(\phi_1/\psi_1, \ldots, \phi_n/\psi_n)$, since it is a possibly repeated application of the first clause of /. R2–R4 easily follow by definition of the unit $1_s : s \to s$, which is a proof term without rule (or composition) symbol. □

Corollary 4.4.6. *Orthogonal rewrite systems are confluent.*

Proof. By Lemma 4.4.4 the ARS $\twoheadrightarrow\!\!\!\!\!\!\!+\;\;$ was shown to posses the diamond property for orthogonal steps, where the function / posed a witness. Now, let $\to$ be an orthogonal rewrite system. By Corollary 4.1.11 $\to \subseteq \twoheadrightarrow\!\!\!\!\!\!\!+\;\; \subseteq \geq_{\mathcal{T}} = \to^*$, where the last equality follows from Theorem 4.1.7. Confluence then is a direct consequence of Proposition 2.2.12. □

From Corollary 4.4.6 above we see that confluence of orthogonal rewrite systems already follows from Lemma 4.4.4. That the residuation of a residual system indeed only performed the steps (or tasks) necessary follows from Lemma 4.4.5, but has not been made explicit yet. Hence, to understand that we have to go into greater detail.

Van Oostrom and de Vrijer introduced residual systems in the context of projection equivalence [23, 28]. Intuitively, it describes the equivalence when the collection of tasks is contained in another collection and vice versa.

Definition 4.4.7. Let $\langle \to, 1, / \rangle$ be a residual system. The *projection* order $\lesssim$ and the corresponding *projection* equivalence $\simeq$ are defined by

$$\phi \lesssim \psi \text{ if } \phi/\psi = 1$$
$$\phi \simeq \psi \text{ if } \phi \lesssim \psi \text{ and } \psi \lesssim \phi$$

for co-initial steps ϕ, ψ.

For the projection order transitivity and reflexivity follow from R1 and R2, respectively. Hence, it defines a quasi-order.

Lemma 4.4.8. *The projection order $\lesssim$ defined by a residual system $\langle \to, 1, / \rangle$ is reflexive and transitive.*

Proof. By R2 it holds that $\phi/\phi = 1$ implying $\phi \lesssim \phi$, i.e., $\lesssim$ is reflexive. Furthermore, if $\phi \lesssim \psi$ and $\psi \lesssim \chi$ it holds that $\phi/\psi = 1$ as well as $\psi/\chi = 1$. Thus,

$$\phi/\chi = (\phi/\chi)/1 = (\phi/\chi)/(\psi/\chi) = (\phi/\psi)/(\chi/\psi) = 1/(\chi/\psi) = 1,$$

where the first equality follows from R3, the third from R1 and the last from R4. □

Nonetheless, the following example shows that the projection order is not a partial order, as it is in general not anti-symmetric.

Example 4.4.9. Consider the TRS defined by $\{\rho : f(x) \to c, \varsigma : a \to b\}$. The system is orthogonal as it is left-linear and rules consist of single and pairwise distinct function symbols. Moreover, consider the co-initial and co-final multi-steps $\rho(a) : f(a) \to c$ and $\rho(\varsigma) : f(a) \to c$. Then, $\rho(a)/\rho(\varsigma) = 1$ and $\rho(\varsigma)/\rho(a) = 1$ implying $\rho(a) \lesssim \rho(\varsigma)$ and $\rho(\varsigma) \lesssim \rho(a)$ for the residuation defined in Lemma 4.4.4 despite the two proof terms being distinct.

However, for every quasi-order $\lesssim$ there exists a partial order by identifying x with y, if $x \lesssim y \,\wedge\, y \lesssim x$. And as the projection equivalence is an equivalence relation, which easily follows by Lemma 4.4.8, we obtain a partial order identifying projection equivalent proof terms. We will not go into further details here but refer to [23, Section 8.7.2]. More important to us is the following definition of join, using the projection order.

Definition 4.4.10. The *join* is a step $\phi \sqcup \psi$ such that

- $\phi \lesssim \phi \sqcup \psi$ and $\psi \lesssim \phi \sqcup \psi$, i.e., the join is an *upper bound* of ϕ, ψ,

- $\phi \sqcup \psi \lesssim \chi$ for all upper bounds χ of ϕ, ψ, i.e., it is the *least* upper bound.

for two steps ϕ, ψ.

Nevertheless, for a residual system joins need not exist as the following example shows.

Example 4.4.11. The TRS defined by $\{\rho : f(x) \to g(x,x), \varsigma : a \to b\}$ is orthogonal for the same reason as the TRS from Example 4.4.9 is. The two parallel steps $\rho(a) : f(a) \twoheadrightarrow g(a,a)$ and $f(\varsigma) : f(a) \twoheadrightarrow f(b)$ are co-initial. We can complete the diamond by the two co-final steps $g(\varsigma,\varsigma) : g(a,a) \twoheadrightarrow g(b,b)$ and $\rho(b) : f(b) \twoheadrightarrow g(b,b)$ but no step from $f(a)$ to $g(b,b)$ exists.

Note that for above example the join exists, if we consider multi-step rewriting. The proof term given by $\rho(\varsigma) : f(a) \multimap g(b,b)$ is a witness to the join. But we can turn every residual system into a residual system, such that joins exist.

Definition 4.4.12. A residual system *with composition* is a quadruple $\langle \to, 1, /, \cdot \rangle$ such that $\langle \to, 1, / \rangle$ is a residual system and $\cdot$ is a binary operation on composable steps satisfying the composition identities:

$$1 \cdot 1 \approx 1 \tag{C1}$$

$$\chi/(\psi \cdot \phi) \approx (\chi/\psi)/\phi \tag{C2}$$

$$(\chi \cdot \psi)/\phi \approx (\chi/\phi) \cdot (\psi/(\phi/\chi)) \tag{C3}$$

The *designated join* $\phi \sqcup \psi$ is defined as $\phi \cdot (\psi/\phi)$.

Theorem 4.4.13. *For a residual system with composition $\langle \to, 1, /, \cdot \rangle$ joins exist and are projection equivalent to the designated join.*

Proof. Obviously, $\phi \lesssim \phi \cdot (\psi/\phi)$ as

$$\begin{aligned} \phi/(\phi \cdot (\psi/\phi)) &= (\phi/\phi)/(\psi/\phi) \\ &= 1/(\psi/\phi) \\ &= 1 \end{aligned}$$

due to C2 for the first equality and R2 and R4 for the second and third equality, respectively. Similarly, $\psi \lesssim \phi \cdot (\psi/\phi)$ as

$$\begin{aligned} \psi/(\phi \cdot (\psi/\phi)) &= (\psi/\phi) \cdot (\psi/\phi) \\ &= 1 \end{aligned}$$

due to C1 and R2. Hence, the designated join is an upper bound for ϕ and ψ. Let χ be a further upper bound, then $\phi/\chi = 1$ and $\psi/\chi = 1$. We show that the designated join is at least as small as χ.

$$\begin{aligned} (\phi \cdot (\psi/\phi))/\chi &= (\phi/\chi) \cdot ((\psi/\phi)/(\chi/\phi)) \\ &= 1 \cdot ((\psi/\phi)/(\chi/\phi)) \\ &= 1 \cdot ((\psi/\chi)/(\phi/\chi)) \\ &= 1 \cdot (1 \cdot 1) \\ &= 1 \end{aligned}$$

where C3, R1 and C1 was applied to the first, third and fifth equation, respectively. The remaining equalities are consequences of χ being an upper bound to ϕ and ψ. Thus, the designated join is a least upper bound and if χ is least as well it is projection equivalent to the designated join. □

Hence, coming back to the example of orthogonal systems Theorem 4.4.13 proved that the residuation defined in Lemma 4.4.4 indeed defines a *least* skolem function, which was shown in Lemma 4.4.5 as it defines a residual system. Intuitively, the residuation provided only as many tasks as necessary.

From the cube law, the unit identities, and from the composition identities we can infer many properties for residual systems.

Corollary 4.4.14. *For a residual system the following holds:*

$$\begin{aligned} \chi/(\phi \sqcup \psi) &= (\chi/\phi)/(\psi/\phi) \\ \chi/(\phi \sqcup \psi) &= \chi/(\psi \sqcup \phi) \\ (\phi \sqcup \psi)/\chi &= (\phi/\chi) \sqcup (\psi/\chi) \end{aligned}$$

with ϕ, ψ, χ co-initial.

Proof. Follows by the definition of designated join as well as C2 and R1. □

Remark 4.4.15. We call the identities of Corollary 4.4.14 the residual cube laws.

Summarizing residuation provides upper bounds, residual systems provide a least upper bound and for any residual system the extension on composable steps exists and has joins.

5 Comprehensive Examples of Residual Systems

The following chapter discusses comprehensive examples of residual systems showing similarities to self-distributivity. It provides the opportunity to abstract from these similarities and derive a residual system for self-distributivity. The examples comprise three rewrite systems: The S-combinator of combinatory logic, associativity and braids. These examples are relevant for our purposes, since the S-combinator bears a syntactic resemblance in the target to self-distributivity, and since associativity has a syntactic correspondence in the source. Furthermore, braids have a close proximity to self-distributivity as Dehornoy extensively examines in his monograph [8]. With the last example we will see that residual systems extend beyond term rewriting as we will formulate braiding via an abstract rewrite system.

5.1 The S-Combinator

An omnipresent example of an orthogonal TRS is Combinatory Logic (CL) invented by Moses Schönfinkel [21]. The signature of CL consists of a binary symbol $*$ and three constants S, K, I together with the rules

$$
\begin{aligned}
*(I, x) &\to x \\
((K, x), y) &\to y \\
((*(S, x), y), z) &\to *(*(x, z), *(y, z))
\end{aligned}
$$

For simplicity we use the binary symbol in an implicit infix notation and associate to the left, e.g., we write $Sxyz$ for $*(*(*(S,x),y),z)$. Due to the similarity to self-distributivity on the right-hand side the last rule is of particular interest. Thus, for the remainder of this section we will consider the TRS $\mathcal{T}_S$ containing the signature $\Sigma_S := \{*, S\}$ and the single rule

$$\rho : Sxyz \to xz(yz).$$

That this system is not terminating is well-known, as for example is shown by Waldmann [29]. Left-linearity is obvious. We do not prove orthogonality but we show only that the function / defined in Lemma 4.4.4 is well-defined for multi-steps $\multimap\!\!\!\to_{\mathcal{T}_S}$. Let $\mathrm{src}(\phi) = s = \mathrm{src}(\psi)$ and assume $\phi = \rho(\phi_1, \phi_2, \phi_3)$. There exist four rule based function symbol occurrences of ϕ in s. These are $o_1 = \langle * \mid \Box\rangle$, $o_2 = \langle * \mid\ *(\Box, \mathrm{src}(\phi_3))\rangle$, $o_3 = \langle * \mid\ *(*(\Box, \mathrm{src}(\phi_2)), \mathrm{src}(\phi_3))\rangle$ and $o_4 = \langle S \mid\ *(*(*(\Box, \mathrm{src}(\phi_1)), \mathrm{src}(\phi_2)), \mathrm{src}(\phi_3))\rangle$. If the occurrence o_1 is also rule-based according to ψ the last case applies as $\psi =$

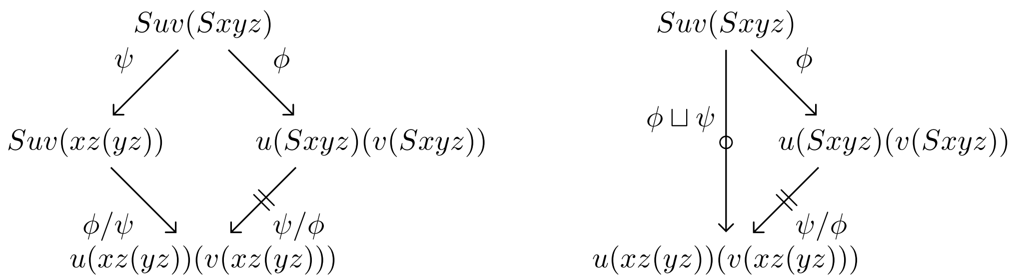


Figure 5.1: The two co-initial single-steps $\phi = \rho(u, v, Sxyz)$ as well as $\psi = Suv\rho(x, y, z))$ with their corresponding residuals $\phi/\psi = \rho(u, v, xz(yz))$ as well as $\psi/\phi = u\rho(x, y, z)(v\rho(x, y, z))$ in $\langle \twoheadrightarrow\!\!\!\!\!\!\not\;\,_{\mathcal{T}_S}, 1, / \rangle$ and $\langle \multimap_{\mathcal{T}_S}, 1, / \rangle$, respectively (*left*). Triangulation via the join of multi-steps displayed at an example of ϕ, ψ (*right*).

$\rho(\psi_1, \psi_2, \psi_3)$. If the occurrence o_2 is rule-based according to ψ but not o_1 it holds that $\psi = *(\rho(\psi_1, \psi_2, \psi_3), \phi_3)$. Nonetheless, $*(*(*(*(S, x^\tau), y^\tau), z^\tau), z^\sigma) \neq *(*(*(S, x^\sigma), y^\sigma), z^\sigma)$ for any substitutions σ, τ as the term structures are different. But the left side of the equation is the source of ϕ for some substitution σ and the right side is the source of ψ for some τ. Similarly for o_3, o_4, i.e., either none or all of $o_1, \ldots, o_4$ are rule-based in ψ. If neither of $o_1, \ldots, o_4$ are rule-based ψ is of the form $\psi = \ell(\psi_1, \psi_2, \psi_3)$ as ψ is co-initial to ϕ. Hence, the second case applies. If $\phi = *(\phi_1, \phi_2)$ either $\psi = *(\psi_1, \psi_2)$ or $\psi = \rho(\psi_1, \psi_2, \psi_3)$. In the former the first case applies and the latter case is symmetric to the explanation above. As a consequence / is well-defined for multi-steps of $\mathcal{T}_S$. However, it is not obvious that / also defines a residuation. The next example gives a first hint that this is still the case.

Example 5.1.1. Consider the following co-initial proof terms

$$\phi = \rho(u, v, Sxyz) : Suv(Sxyz) \to_{\mathcal{T}_S} u(Sxyz)(v(Sxyz))$$
$$\psi = Suv\rho(x, y, z) : Suv(Sxyz) \to_{\mathcal{T}_S} Suv(xz(yz)).$$

The function / from Lemma 4.4.4 provides us with the residuals

$$\psi/\phi = u\rho(x, y, z)(v\rho(x, y, z)) : u(Sxyz)(v(Sxyz)) \twoheadrightarrow\!\!\!\!\!\!\not\;\,_{\mathcal{T}_S} u(xz(yz))(v(xz(yz)))$$
$$\phi/\psi = \rho(u, v, xz(yz)) : Suv(xz(yz)) \to_{\mathcal{T}_S} u(xz(yz))(v(xz(yz)))$$

(see Figure 5.1 left).

For showing that the function / defined in Lemma 4.4.4 is indeed a residuation we do make use of Lemma 4.4.4, but present a different proof here. Namely, instead of showing that the residuation builds a diamond we can triangulate by defining a commutative upper bound, which we call join. Then, we show that the target of the residuation is the target of the join. By commutativity the diamond property follows. However, with

Example 5.1.4 we will see that this approach only works for multi-steps. We could have presented this method in Section 4.4, since it holds for orthogonal multi-steps in general, but nonetheless we only present it here to support it with examples of the S-combinator illustrating the bit we will abstract from in Chapter 6. Note that we show the following for orthogonal steps in general. For the case of $\mathcal{T}_S$ we have not shown orthogonality. But preceding proofs apply also for $\mathcal{T}_S$ as they depend on the clauses of /, which we have shown to be well-defined for $\mathcal{T}_S$.

Definition 5.1.2. For co-initial and orthogonal multi-steps ϕ, ψ the *join* is defined as

$$\phi \sqcup \psi := \begin{cases} f(\phi_1 \sqcup \psi_1, \ldots, \phi_n \sqcup \psi_n) & \text{if } \phi = f(\phi_1, \ldots, \phi_n), \psi = f(\psi_1, \ldots, \psi_n) \\ \rho(\phi_1 \sqcup \psi_1, \ldots, \phi_n \sqcup \psi_n) & \text{if } \phi = \rho(\phi_1, \ldots, \phi_n), \psi = \ell(\psi_1, \ldots, \psi_n) \\ \rho(\phi_1 \sqcup \psi_1, \ldots, \phi_n \sqcup \psi_n) & \text{if } \phi = \ell(\phi_1, \ldots, \phi_n), \ \psi = \rho(\psi_1, \ldots, \psi_n) \\ \rho(\phi_1 \sqcup \psi_1, \ldots, \phi_n \sqcup \psi_n) & \text{if } \phi = \rho(\phi_1, \ldots, \phi_n), \psi = \rho(\psi_1, \ldots, \psi_n) \end{cases}$$

The notion of join is well-defined, since ϕ, ψ do not share a rule-based function symbol occurrence as ϕ and ψ are orthogonal. By symmetry in the definition the join is commutative.

Lemma 5.1.3. *For co-initial, orthogonal multi-steps ϕ, ψ the join $\phi \sqcup \psi$ is a multi-step and the following holds:*

$$\begin{aligned} src(\phi) &= src(\phi \sqcup \psi) \\ tgt(\psi/\phi) &= tgt(\phi \sqcup \psi). \end{aligned}$$

Proof. That the join is again a multi-step is proven by a structural induction on the clauses of the definition of $\sqcup$. The equalities follow by another structural induction and the definition of / in Lemma 4.4.4 combined with the easy observation that $\mathrm{src}(\rho(\phi_1, \ldots, \phi_n)) = \mathrm{src}(\ell(\phi_1, \ldots, \phi_n))$ as well as $\mathrm{tgt}(\rho(\phi_1, \ldots, \phi_n)) = \mathrm{tgt}(r(\phi_1, \ldots, \phi_n))$. ☐

That multi-steps fulfil the diamond property is a direct consequence of Lemma 5.1.3 and the join being commutative. Therefore, / is a residuation for multi-steps, which to show was the goal of this detour. Note, as the following example illustrates that the join of two parallel steps is in general not a parallel step.

Example 5.1.4. Let ϕ, ψ be as of Example 5.1.1. The join is then given by $\phi \sqcup \psi = \rho(u, v, \rho(x, y, z)) : Suv(Sxyz) \multimap\!\!\!\!\circ\!\!\!\rightarrow_{\mathcal{T}_S} u(xz(yz))(v(xz(yz)))$ (see Figure 5.1 right). Since ϕ, ψ are single-steps, they also are parallel steps and multi-steps. However, the join is no parallel step as it contains nested rule symbols.

With the clauses defining / being well-defined for $\multimap\!\!\!\!\circ\!\!\!\rightarrow_{\mathcal{T}_S}$ the triple $\langle \multimap\!\!\!\!\circ\!\!\!\rightarrow_{\mathcal{T}_S}, 1, / \rangle$ can be proven to fulfil R1–R4 in the same way as was done in the proof of Lemma 4.4.5. Hence, it defines a residual system and / provides the *least* co-final multi-steps. Confluence of the S-combinator follows accordingly to the proof of Corollary 4.4.6 exchanging $\multimap\!\!\!\!\parallel\!\!\!\rightarrow$ with $\multimap\!\!\!\!\circ\!\!\!\rightarrow$.

5.2 Associativity

Consider the term rewriting system over the signature $\Sigma_{\mathcal{A}}$ consisting of a single binary function symbol $*$ with the ARS $R_{\mathcal{A}}$ containing the only rule

$$\rho : *(*(x, y), z) \to *(x, *(y, z)).$$

We define the TRS by $\mathcal{T}_{\mathcal{A}}$ and refer to it as *associativity.* We adopt notation from Section 5.1 and may use implicit infix notation for $*$. Furthermore, we assume that $*$ associates to the left, to improve readability. Moreover, we infer the arity of ρ, i.e.,

$$\rho(x, y, z) : \ell(x, y, z) \to r(x, y, z)$$

with $\ell(x, y, z) = xyz$ and $r(x, y, z) = x(yz)$. Similar to the S-combinator associativity is left-linear. However, a significant difference to the S-combinator is that associativity is not orthogonal. Two proof terms witnessing non-orthogonality are the following,

$$\rho(*(w, x), y, z) : wxyz \to_{\mathcal{T}_{\mathcal{A}}} wx(yz)$$
$$*(\rho(w, x, y), z) : wxyz \to_{\mathcal{T}_{\mathcal{A}}} w(xy)z$$

representing co-initial single-steps, since they have exactly one occurrence of a rule symbol and the same source. Nonetheless, their patterns result in

$$\rho(\square, \square, \square) : \square\square\square \to_{\mathcal{T}_{\mathcal{A}}} \square(\square\square)$$
$$*(\rho(\square, \square, \square), z) : \square\square\square z \to_{\mathcal{T}_{\mathcal{A}}} \square(\square\square)z$$

and the function symbol occurrence $\langle * \mid *(\square, z)\rangle$ is rule-based in both, since it (implicitly) appears in the sources but in neither proof term itself and, furthermore, the sources of the patterns aren't prefixes of $\square z$, i.e., neither $\square\square\square$ nor $\square\square\square z$ is a prefix of $\square z$. Hence, we do not have a residual system given by Lemma 4.4.5.

In the remainder of this section we will derive two residual systems for associativity. The difference between the two being that the first one will not and the second one will have joins. Both constructions go back to van Oostrom [26]. Similarities can be drawn to an approach by Melliès [16].

Note that $\mathcal{T}_{\mathcal{A}}$ does not posses the diamond property as Figure 5.2 shows. Hence, we have to enrich the system by further steps. Only adding the step from $w(xy)z$ to $w(x(yz))$ to form a diamond in Figure 5.2 is not enough, as new diagrams not forming a diamond arise. Making these new diagram into diamonds as well is called faceting in terminology of van Oostrom. This describes the process quite well as we merge multiple edges of a polygon into a single facet to form a diamond. In the case of associativity this process does not stop, but still the new rules generated adhere to a regular pattern, resulting in the following TRS having infinitely many rules.

Definition 5.2.1. Define by $\mathcal{T}'_{\mathcal{A}} = (\Sigma_{\mathcal{A}}, R'_{\mathcal{A}})$ where $R'_{\mathcal{A}}$ consists for each $n \in \mathbb{N} \setminus \{0\}$ of a rule

$$\rho_n : \ell_n \to r_n$$

with $\ell_n = x_1(x_2(\dots(x_n y)\dots))z$ and $r_n = x_1(x_2(\dots(x_n(yz))\dots))$.

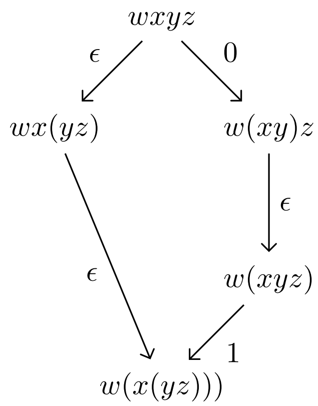


Figure 5.2: Joining two co-initial, overlapping single-steps of the associativity rule. Arrows indicating the position where ρ was applied.

Remark 5.2.2. See Figure 5.3 for a visualization of ρ_n. On the one hand, $\rho_1 : \ell_1 \to r_1 \in R'_{\mathcal{A}}$ corresponds to $\rho : \ell \to r \in R_{\mathcal{A}}$, since $\ell_1 \equiv \ell$ and $r_1 \equiv r$. On the other hand, we can simulate $\rho_n : \ell_n \to r_n \in R'_{\mathcal{A}}$ by a proof term $\phi : s \geq_{\mathcal{T}_{\mathcal{A}}} t$, namely by

$$\rho(x_1, *(x_2, *(x_3, *(\ldots, *(x_n, y) \ldots))), z) \cdot *(x_1, \rho(x_2, *(x_3, *(\ldots, *(x_n, y) \ldots)), z)) \\ \cdot \ldots \cdot *(x_1, *(x_2, *(\cdots * (x_{n-1}, \rho(x_n, y, z)))))$$

such that $\ell_n = s$ and $r_n = t$, i.e., ρ_n can be seen as an n-times repeated application of ρ.

Notation 5.2.3. To match the variable naming of Definition 5.2.1 we will use $x_1, \ldots, x_n, y, z$ for the $n+2$ variables in $\rho_n : \ell_n \to r_n \in R'_{\mathcal{A}}$. Furthermore, to avoid notational clutter we introduce $\bar{x}^\sigma_n$ as abbreviation for $x^\sigma_1, \ldots, x^\sigma_n$ and $\bar{x}^\sigma_{i,j}$ as abbreviation for the interval $x^\sigma_i, \ldots, x^\sigma_j$, where σ is a substitution.

Lemma 5.2.4. $\to_{\mathcal{T}'_{\mathcal{A}}}$ *together with a trivial step* 1 *has the diamond property.*

Proof. Let $\phi : s \to_{\mathcal{T}'_{\mathcal{A}}} t_1, \psi : s \to_{\mathcal{T}'_{\mathcal{A}}} t_2$ be co-inital single-steps overlapping due to ρ_n in ϕ and due to ρ_m in ψ. Note, that by the definition of ρ_n there exist $n+1$ rule-based function symbol occurrences of ϕ in s. Denote by $\langle * \mid C_0[\ ] \rangle$ the outermost rule-based function symbol occurrence of ϕ, i.e., for all other rule-based function symbol occurrences $\langle * \mid C_i[\ ] \rangle$ of ϕ, $0 < i \leq n$, the context $C_0[\ ]$ is a prefix of $C_i[\ ]$. The context $C_0[\ ]$ is well-defined, since the ρ_n-redex is a sub-term of s. Furthermore, let

$$C_1[\ ] = C_0[*(\Box, z^\sigma)]$$
$$C_{i+1}[\ ] = C_i[*(x^\sigma_{i-1}, \Box)] \text{ for } 1 \leq i \leq n-1$$

for a substitution σ. Similarly, there exist $m+1$ rule-based function symbol occurrences in s of ψ, which we denote in the same pattern as for the $C'_i s$ by $\langle * \mid D_i[\ ] \rangle$, with $0 \leq i \leq m$, for a substitution τ. Since ϕ and ψ overlap, there exist $0 \leq k \leq n$, such that $C_k[\ ] = D_0[\ ]$. For readability but without loss of generality assume $C_0[\ ] = \Box$ and do a case distinction on k (see Figure 5.4).

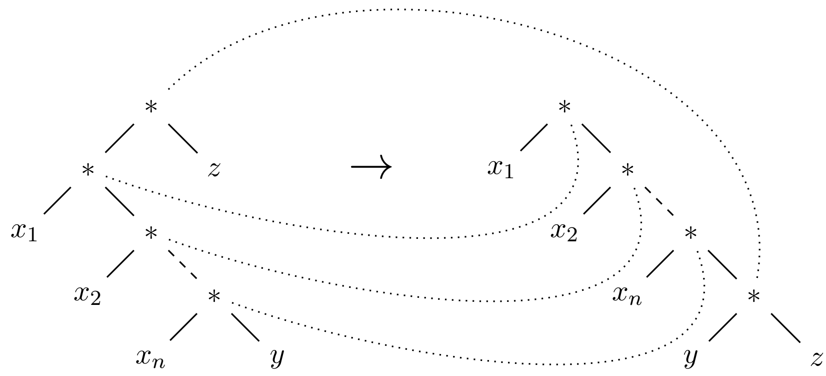


Figure 5.3: Source and target of a rule ρ_n in $\mathcal{T}'_{\mathcal{A}}$ as term trees and the corresponding rule tracing $[\rho_n\rangle$ indicated by dotted lines.

- Case $k = 0$. Without loss of generality let $n < m$, then $\phi = \rho_n(\bar{x}^\tau_n, *(x^\tau_{n+1}, *(\cdots * (x^\tau_m, y^\tau)\cdots)), z^\tau)$ and $\psi = \rho_m(\bar{x}^\tau_m, y^\tau, z^\tau)$. The diamond is completed by

$$\phi' = *(x^\tau_1, *(\cdots * (x^\tau_n, \rho_{m-n}(\bar{x}^\tau_{n+1,m}, y^\tau, z^\tau))\cdots))$$

and the trivial step $\psi' = 1$. Note that $x^\sigma_i = x^\tau_i$ for $0 \le i \le n$ and $z^\sigma = z^\tau$.

- Case $0 < k \le n$. Then $\phi = \rho_n(\bar{x}^\sigma_{k-1}, *(x^\tau_1, *(\cdots * (x^\tau_m, y^\tau)\cdots), \bar{x}^\sigma_{k+1,n}, y^\sigma, z^\sigma)$ and $\psi = *(*(x^\sigma_1, *(\cdots * (x^\sigma_{k-1}, \rho_m(\bar{x}^\tau_m, y^\tau, *(x^\sigma_{k+1}, *(\cdots * (x^\sigma_n, y^\sigma)\cdots))))\cdots)), z^\sigma)$. The diamond is completed by

$$\phi' = *(x^\sigma_1, *(\cdots * (x^\sigma_{k-1}, \rho_m(\bar{x}^\tau_m, y^\tau, *(x^\sigma_{k+1}, *(\cdots * (x^\sigma_n, *(y^\sigma, z^\sigma))\cdots)))\cdots))$$

and $\psi' = \rho_{n+m}(\bar{x}^\sigma_{k-1}, \bar{x}^\tau_m, y^\tau, \bar{x}_{k+1,n}, y^\sigma, z^\sigma)$.

In the case where ϕ, ψ do not overlap, Lemma 4.4.4 provides us with $\phi' = \psi/\phi$ and $\phi' = \phi/\psi$ completing the diamonds, since ϕ, ψ are single-steps and consequently also multi-steps. □

To show that not only the diamond property but also the cube property holds, we interpret associativity in its trace algebra. Define for $\rho_n : \ell_n \to r_n$ the rule tracing $[\rho_n\rangle = \{(\epsilon, 1^n), (01^k, 1^k), (01^k0, 1^k0), (01^n, 1^n0), (1, 1^{n+1}) \mid 0 \le k < n\}$ (see Figure 5.3). Hence, for a single-step $\phi : s \to_{\mathcal{T}'_{\mathcal{A}}} t$ and $P = \{[\rho_n\rangle \mid \rho_n \in R_{\mathcal{A}}\}$ the interpretation $[[\phi\rangle\rangle_P$ defines its trace relation. Now, note that a single-step $\phi = C[\rho_n(\bar{x}^\sigma_n, y^\sigma, z^\sigma)]$ is determined by the pair $(p, p01^n)$, where p denotes the position of the hole in the context $C[\ ]$ and n corresponds to the number of x_i-variables in the corresponding rule ρ_n. Then $p01^n$ defines the position of the y-variable. Subsequently, we will use this characterization for steps.

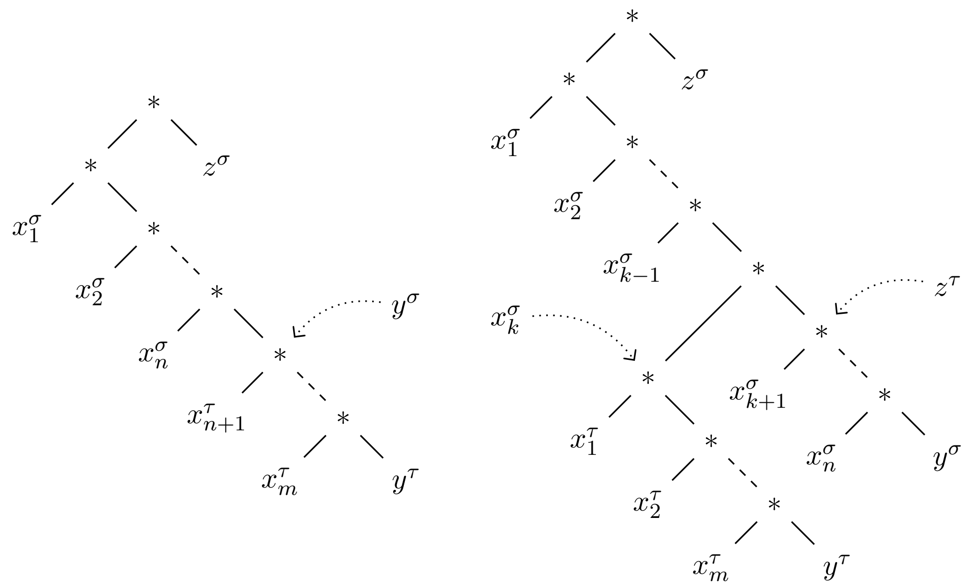


Figure 5.4: Comparing the cases of overlap in $\mathcal{T}'_{\mathcal{A}}$ together with a trivial step 1 for the single-steps consisting of $\rho_n(\bar{x}_n^\sigma, y^\sigma, z^\sigma)$ and $\rho_m(\bar{x}_m^\tau, y^\tau, z^\tau)$, respectively. Here, the left term tree resembles the case $k = 0$, i.e., the overlap at the function symbol occurrence $\langle * \mid \Box \rangle$ and the right term tree resembles the case $0 < k \leq n$, i.e., the overlap at the function symbol occurrence $\langle * \mid C_k[\ ] \rangle$ (see Proof of Lemma 5.2.4 for the definition of $C_k[\ ]$).

Example 5.2.5. Let ϕ correspond to the pair $(\epsilon, 011)$. The trace relation of ϕ is given by

$$[[\epsilon, 011\rangle\rangle = \{(\epsilon, 11), (0, \epsilon), (01, 1), (00q, 0q), (010q, 10q), (011, 110), (1q, 111q) \mid q \in \mathcal{P}os\}.$$

Let ψ correspond to the pair $(p, p01^n)$ with $p \in \mathcal{P}os$. The set of tuples

$$[[p, p01^n\rangle\rangle = \{(p, p1^n), (p01^k, p1^k), (p01^k0q, p1^k0q), (p01^nq, p1^n10q), (p1q, p1^{n+1}q), (r, r) \mid q, r \in \mathcal{P}os, p \not\sqsubseteq r, 0 \leq k < n\}.$$

defines the trace relation of ψ.

With the knowledge we gained from proving the diamond property for $\mathcal{T}'_{\mathcal{A}}$ we define a residuation. Afterwards we show in the first theorem of this section that this residuation also defines a residual system for $\to_{\mathcal{T}'_{\mathcal{A}}}$ together with a trivial step. See Notation 2.1.1 denoting elements in the codomain of a relation.

Lemma 5.2.6. *Let ϕ correspond to the pair $(p, p01^n)$ and ψ correspond to $(q, q01^m)$. The function $/_{\mathcal{A}}$ defined by*

$$\psi /_{\mathcal{A}} \phi := (q\ [[p, p01^n\rangle\rangle, q01^m\ [[p, p01^n\rangle\rangle),$$

where we define the right-hand side as 1*, if it is not of the required shape for a step, is a residuation for $\to_{\mathcal{T}'_{\mathcal{A}}}$.*

Proof. If $p = q$ the steps ϕ, ψ overlap and, thus, the residual is given by $\psi /_{\mathcal{A}} \phi = (p1^n, p1^n01^{m \dot{-} n})$.[1] This reflects the case $k = 0$ in the proof of Lemma 5.2.4. Note that in case $n \geq m$ the residual is not of required shape, hence, the residual denotes the trivial step. If $q = p01^k$ the residual is given by $(p01^k, p01^k01^m) /_{\mathcal{A}} (p, p01^n) = (p1^k, p1^k01^m)$ corresponding to the overlap case $0 < k \leq n$ of Lemma 5.2.4 and to the residual given by Lemma 4.4.4 if $k > n$. If $p = q01^k$ we have to distinguish between $0 < k \leq m$, where $(q, q01^m) /_{\mathcal{A}} (q01^k, q01^k01^n) = (p, p01^{n+m})$ reflecting the respective overlapping case, in Lemma 5.2.4 and between $k > m$, where $(q, q01^m) /_{\mathcal{A}} (q01^k, q01^k01^n) = (q, q01^m)$ corresponds to the residual in Lemma 4.4.4. If neither $p \sqsubseteq q$ nor $q \sqsubseteq p$ the steps ϕ and ψ are horizontally orthogonal and we get $\psi /_{\mathcal{A}} \phi = (q, q01^m)$, which reflects Lemma 4.4.4. Hence, $\text{tgt}(\phi) = \text{src}(\psi /_{\mathcal{A}} \phi)$ and $\text{tgt}(\phi /_{\mathcal{A}} \psi) = \text{tgt}(\psi /_{\mathcal{A}} \phi)$, which shows the claim. □

Theorem 5.2.7. $\langle \to_{\mathcal{T}'_{\mathcal{A}}}, 1, /_{\mathcal{A}} \rangle$ *constitutes a residual system for the residuation $/_{\mathcal{A}}$ defined in Lemma 5.2.6.*

Proof. The laws R2–R4 from the residual identities are trivial. To see that the cube identity R1 also holds note that we defined for each ρ_n a rule tracing and showed in Lemma 5.2.6 that the corresponding proof term algebra $\mathfrak{A}$ is a model for the diamonds, i.e., $\psi \cdot (\chi/\psi) =_{\mathfrak{A}} \chi \cdot (\psi/\chi)$ with ψ, χ co-initial in $\to_{\mathcal{T}'_{\mathcal{A}}}$. Take ϕ co-initial to ψ, χ and trace its position pair (p_1, p_2) along the right and left path of a diamond. Obviously, $p_i\ [[\psi\rangle\rangle \cdot [[\chi/\psi\rangle\rangle\ p'_i$ and $p_i\ [[\chi\rangle\rangle \cdot [[\psi/\chi\rangle\rangle\ p'_i$ for $i \in \{1, 2\}$. Hence, contracting ϕ after either path results in the same relation, i.e., $(\phi/\psi)/(\chi/\psi) =_{\mathfrak{A}} (\phi/\chi)/(\psi/\chi)$ (compare Figure 5.5). □

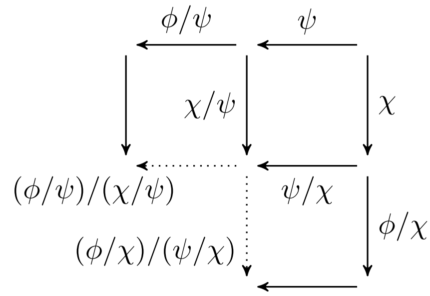


Figure 5.5: Tracing the position pair of ϕ's redex-pattern in $\mathcal{T}'_{\mathcal{A}}$ results in the same position pair along the left and right path of the diamond representing a redex-pattern again. Hence, contracting the residual of ϕ after either path results in the same step, i.e., the dotted lines must coincide.

Concluding we may note that the residual system $\langle \rightarrow_{\mathcal{T}'_{\mathcal{A}}}, 1, / \rangle$ does not have diagonals, i.e., the designated join of the corresponding residual system with composition is not a single-step. This is witnessed by the following example.

Example 5.2.8. Let $\phi = \rho_1(*(x_1, x_2), y, z) : x_1x_2yz \rightarrow_{\mathcal{T}'_{\mathcal{A}}} x_1x_2(yz)$, as well as $\psi = \rho_1(x_1, x_2, *(y, z)) : x_1x_2yz \rightarrow_{\mathcal{T}'_{\mathcal{A}}} x_1(x_2y)z$, which correspond to the representation $(\epsilon, 01)$ and $(0, 001)$ respectively. The residuals are computed by

$$\phi/\psi = (\epsilon, 01)/(0, 001) = (\epsilon[[0, 001\rangle\rangle, 01[[0, 001\rangle\rangle) = (\epsilon, 011),$$
$$\psi/\phi = (0, 001)/(\epsilon, 01) = (0[[\epsilon, 01\rangle\rangle, 001[[\epsilon, 01\rangle\rangle) = (\epsilon, 01),$$

hence, $\phi/\psi = \rho_2(x_1, x_2, y, z) : x_1(x_2y)z \rightarrow_{\mathcal{T}'_{\mathcal{A}}} x_1(x_2(yz))$ and $\psi/\phi = \rho_1(x_1, x_2, *(y, z)) : x_1x_2(yz) \rightarrow_{\mathcal{T}'_{\mathcal{A}}} x_1(x_2(yz))$. Then, the designated join $\phi \sqcup \psi$ is co-initial with ϕ, ψ and co-final with $\phi/\psi, \psi/\phi$ and is given by $\phi \sqcup \psi = \phi \cdot (\psi/\phi) = \rho_1(*(x_1, x_2), y, z) \cdot \rho_1(x_1, x_2, *(y, z)) : x_1x_2yz \geq_{\mathcal{T}'_{\mathcal{A}}} x_1(x_2(yz))$. Note that there exists no co-initial single-step distinct from ϕ and ψ in $\rightarrow_{\mathcal{T}'_{\mathcal{A}}}$, as for ρ_i, $i \geq 2$, the source does not match.

Here, it may be noted that we experience a similar situation in the case of orthogonal TRS's. The triple $\langle \mathrel{\|\!\!\!\twoheadrightarrow}, 1, / \rangle$ constitutes a residual system without diagonals. However, enriching the ARS $\mathrel{\|\!\!\!\twoheadrightarrow}$ by the diagonals results in the ARS $\mathrel{\circ\!\!\!\twoheadrightarrow}$ and the triple $\langle \mathrel{\circ\!\!\!\twoheadrightarrow}, 1, / \rangle$ still constitutes a residual system. Likewise we will proceed with associativity. Hence, to follow suit we will from now on use $\mathrel{\|\!\!\!\twoheadrightarrow}_{\mathcal{A}}$ for $\rightarrow_{\mathcal{T}'_{\mathcal{A}}}$. In the following we will then enrich $\mathrel{\|\!\!\!\twoheadrightarrow}_{\mathcal{A}}$ by its diagonals of the diamonds. The result we will denote by $\mathrel{\circ\!\!\!\twoheadrightarrow}_{\mathcal{A}}$. Doing so we will make use of the findings by Nao Hirokawa et al. defining linear terms (see Definition 2.3.1) as *patterns* and who show that patterns are characterized by non-empty, convex[2] sets of positions [12]. We overload the terminology and adopt this definition for pattern. To avoid confusion with patterns of Definition 4.2.1 we may sometimes call them *positional* patterns. A connection between the two is given by the next definition.

[1]By $\dot{-}$ we denote the cut-off subtraction, also known as *monus*, i.e., $2 \dot{-} 1 = 1$ but $1 \dot{-} 2 = 0$.
[2]A set of positions is defined as convex, if for each pair p, q of positions the shortest path from p to q in the corresponding term tree is entirely contained in the set as well.

Definition 5.2.9. Let $\phi : s \to_{\mathcal{T}} t$ be a single-step with $\mathcal{T}$ left-linear, such that $\phi = C[\rho(x_1, \dots, x_n)]$ for a context $C[\,]$ and a rule $\rho : \ell \to r$. The *redex-pattern* $\mathcal{RP}os(\phi)$ of ϕ is a subset of $\mathcal{P}os(s)$ consisting of all vertex positions $p \cdot q$, such that p is the position of the hole in $C[\,]$ and q is a non-variable position in l.

Hence, the redex-pattern of a single rule is a set of positions containing exactly all rule-based function symbol occurrences, i.e., the redex-pattern of a single-step can be interpreted as the positional pattern of a sub-term defining its redexes pattern in the sense of Definition 4.2.1. Thus, both notions are connected but one describes a term over the proof term signature extended by $\square$ and the other a set of positions. A multipattern is respectively defined as a set of pairwise disjoint positional patterns.

Definition 5.2.10. A *development* of a multipattern η in a term s is co-inductively defined as either the empty step 1 from s or a single ρ-step $\phi : s \to t$, such that $\mathcal{RP}os(\phi) \subseteq P$ with $P \in \eta$, composed with a development of $(\eta\ [[\phi\rangle\rangle)$ in t. Here, $(\eta\ [[\phi\rangle\rangle)$ denotes pointwise tracing of each set in η by $[[\phi\rangle\rangle$. A development is *complete* if there exists no ρ-step ϕ such that $\mathcal{RP}os(\phi) \subseteq P \in \eta$.

Remark 5.2.11. A development is well-defined, since $[[\phi\rangle\rangle$ is a relation on $\mathcal{P}os(s) \times \mathcal{P}os(t)$ for $\phi : s \to t$ ensuring that steps are composable and since $[[\phi\rangle\rangle$ is a bijection securing that patterns stay disjoint. Note that defining developments co-inductively allows infinite developments. Hence, termination of developments needs to be proven.

The next example illustrates the difference of a multipattern consisting of a single pattern and a multipattern comprised of two patterns that unify to the single pattern.

Example 5.2.12. Consider the TRS defined by $\{\rho : f(x) \to g(x), \varsigma : a \to c, \pi : f(a) \to d\}$ and the term $t = f(a)$. Then $\mathcal{P}os(t) = \{\epsilon, 0\}$. Completely developing $\{\{\epsilon\}, \{0\}\}$ results in $g(c)$. Completely developing $\{\{\epsilon, 0\}\}$ results in either $g(c)$ or d.

However, as we are concerned with the sole rule of associativity we only come across multipatterns consisting of a single pattern.

Lemma 5.2.13. *Let ϕ, ψ be proof terms of $\mathcal{T}_{\mathcal{A}}$, such that ϕ, ψ are two complete developments of η in a term s, then $tgt(\phi) = tgt(\psi)$.*

Proof. The system $\mathcal{T}_{\mathcal{A}}$ is complete. Confluence follows from Theorem 5.2.7 and termination can easily be shown, e.g., by the algebra interpreting $*(x, y) = 2x + y + 1$. And, since completely developing a multipattern coincides to computing for each pattern the (unique) normal form of the corresponding pattern over the extended proof term signature the claim follows. $\square$

Definition 5.2.14. Define by $\multimap_{\mathcal{A}} \subseteq \geq_{\mathcal{T}_{\mathcal{A}}}$ the rewrite system consisting of steps defined by multipatterns, where the source and the target of a multipattern η in s are the source and the target of any complete development of η. We write $\eta : s \multimap_{\mathcal{A}} t$ and define a multipattern with patterns comprising of no ρ-step as the empty step.

Remark 5.2.15. The target of a multipattern is well-defined by Lemma 5.2.13. By Theorem 5.2.7 every complete development of a disjoint multipattern η constitutes the same trace relation denoted by $[\eta]$.

Example 5.2.16. Let $\eta = \{\{0, 00, 001\}\}$ and $t = x(yz)wx$, then $\eta \subseteq \mathcal{P}os(t)$. A complete development of η in t is given by

$$*(\rho(x, *(y, z), w), x) \cdot *(*(x, \rho(y, z, w)), x) : x(yz)wx \geq_{\mathcal{T}} x(y(zw))x$$

with intermediate multipattern $\{\{0, 01, 010\}\}$ and resulting multipattern $\{\{0, 01, 011\}\}$. The development is complete since the latter multipattern does not contain a ρ-redex-pattern.

Definition 5.2.17. Let η, ζ be multipatterns.

- The relation $\between \subseteq \eta \times \eta$ is defined by $P \between Q$ if and only if $P \cap Q \neq \emptyset$ for $P, Q \in \eta$.
- $P_{\between} := (P \ \between^{+})$, i.e. the sets connected to $P \in \eta$ in the transitive closure of $\between$.
- The join of η, ζ is defined by $\eta \sqcup \zeta := \{\bigcup P_{\between} \mid P \in \eta \cup \zeta\}$.

In the last item it holds that $\between \subseteq (\eta \cup \zeta) \times (\eta \cup \zeta)$.

Intuitively, the set $P_{\between}$ comprises of all sets connected to P by successive overlap and the join unifies all those successively connected sets in η and ζ.

Example 5.2.18. Let $\eta = \{\{\epsilon, 0, 00\}, \{1, 10\}\}$ and $\zeta = \{\{0, 01\}, \{1, 11\}, \{10, 100, 101\}\}$. The join is then given by $\eta \sqcup \zeta = \{\{\epsilon, 0, 00, 01\}, \{1, 10, 100, 101, 11\}\}$.

Lemma 5.2.19. *Let η, ζ be multipatterns. The function $/_{\mathcal{A}'}$ defined by $\zeta /_{\mathcal{A}'} \eta := (\eta \sqcup \zeta)[\eta]$ is a residuation for $\multimap\!\!\!\rightarrow_{\mathcal{A}}$, where $[\eta]$ is lifted pointwise to sets of positions.*

Proof. First, observe for each pattern in $P \in \eta \cup \zeta$ that P is a sub-term of s, and by the definition of the join there exists a pattern $Q \in \eta \sqcup \zeta$ such that $P \subseteq Q$. Hence, a complete development of η is a (not necessarily complete) development of $\eta \sqcup \zeta$, which implies $\mathrm{tgt}(\eta) = \mathrm{src}((\eta \sqcup \zeta)[\eta])$. Second, observe that $\eta \sqcup \zeta = \zeta \sqcup \eta$ holds by commutativity of set union and by co-finality of complete developments. Consequently, completely developing $(\eta \sqcup \zeta)[\eta]$ and $(\zeta \sqcup \eta)[\zeta]$ result in steps having the same target, namely $\mathrm{tgt}(\eta \sqcup \zeta)$. $\square$

Remark 5.2.20. Since the join $\eta \sqcup \zeta$ contains the patterns of η, ζ such that those patterns having successive overlap are *merged* into one we see that the diagonals of the diamonds are part of $\multimap\!\!\!\rightarrow_{\mathcal{A}}$.

Example 5.2.21. The step $(p, p12^n)$ of the system $\twoheadrightarrow\!\!\!\!\!\!\!\!+\,_{\mathcal{A}}$ corresponds to the multipattern $\{\{p, p1, p12, \ldots, p12^{n \dot{-} 1}\}\}$ of $\multimap\!\!\!\rightarrow_{\mathcal{A}}$. Hence, mapping the one to the other commutes with the respective residuation.

The next theorem is the main statement of this section showing that the above defined residuation indeed satisfies the residual identities.

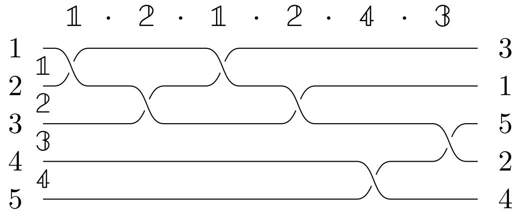


Figure 5.6: A braid with only positive crossings and its corresponding braid word $\mathbb{1} \cdot \mathbb{2} \cdot \mathbb{1} \cdot \mathbb{2} \cdot \mathbb{4} \cdot \mathbb{3}$.

Theorem 5.2.22. $\langle \multimap_{\mathcal{A}}, 1, /_{\mathcal{A}'} \rangle$ *constitutes a residual system for the residuation* $/_{\mathcal{A}'}$ *defined in 5.2.19.*

Proof. We will proceed similar to the proof of Theorem 5.2.7. R2–R4 are trivial. To see that R1 also holds recall from Remark 5.2.15, that each multipattern induces a trace relation and that the corresponding proof term algebra is by Lemma 5.2.19 a model for the diamonds. Meaning, the residuals of a multipattern along either path of a diamond are equal. □

5.3 Braids

In the preceding sections we saw a residual system for the S-combinator and for associativity. The former represents a syntactic orthogonal system. The latter on the other hand was shown to have overlap and is hence not orthogonal in the syntactic sense but semantic sense. In the upcoming section we will investigate a residual system for braids. Meaning the interpretation of orthogonality via residual systems can be extended beyond term rewriting as braids do not have a term structure. This differs from Section 5.1 and 5.2, as the comprehensive examples discussed there are based on term rewrite systems. Nonetheless, by Dehornoy braids have a close proximity to self-distributivity [8]. Examining their residual structures shows us in particular the importance of scopic relations, which play an substantial role with respect to self-distributivity as well.

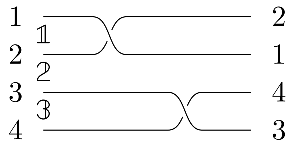
Braids as presented here were introduced by Artin [1]. For a general and more contemporary presentation we refer the interested reader to the works of Dehornoy or Endrullis & Klop [8, 10]. Here, we will only give an introductory overview.

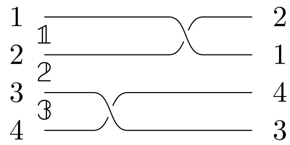
Braids can be viewed as in the conventional way, namely as a set of strands, which cross over each other (see Figure 5.6). The ropes are called strands. Two braids are considered equal if we can continuously transform one braid into the other without intersecting strands. Furthermore, the transformation of the strands is done between two imaginary lines through the start and end points, while these points stay fixed. One can get an easy intuition about this by imagining actual ropes spanned between two walls – one setting for each braid. If we can make them look the same, without cutting ropes and afterwards glueing them together again but only by dragging, we consider them as equal.

Artin discretized their continuous transformations characterizing braids as a string rewrite system. A braid is then represented as a word indicating from left to right in which gap a crossing is performed. A crossing is called positive if in gap $\mathbb{i}$ the i-th strand crosses over the $(i+1)$-st strand (in Figure 5.6 this is equivalent to 'if the upper strand crosses over the lower strand'). A crossing is called negative if the $(i+1)$-fst crosses over the i-th strand and is denoted by $\mathbb{i}^{-1}$. Artin originally considered braids with positive and negative crossings. This section considers braids with positive crossings, but we note that positive braids can be used to generate general braids similar as the natural numbers can be used to generate the integers.

Artin has shown that two simple equations considering braid words are enough to characterize braid equivalences, known as the *positive braid* relations. The formal proof of the characterization can be found in [8, Lemma 1.16]. These relations describe the following.

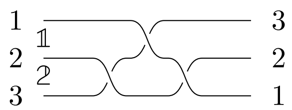
The first equation addresses the fact, that it is not important in which order we perform the crossings on independent pairs of strands, as can be seen below.

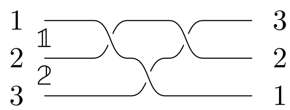




Thus, for $|\mathbb{i} - \mathbb{j}| > 1$ the equation $\mathbb{i} \cdot \mathbb{j} = \mathbb{j} \cdot \mathbb{i}$ holds.

For adjacent gaps, so if $|\mathbb{i} - \mathbb{j}| = 1$, crossings do not commute. But $\mathbb{i} \cdot \mathbb{j} \cdot \mathbb{i} = \mathbb{j} \cdot \mathbb{i} \cdot \mathbb{j}$ holds, which is shown and easily verified by comparing the following two braid diagrams:





Summarizing the above we get the following lemma on Artin's positive braid relations [1].

Lemma 5.3.1. *Two braids are topologically equivalent if and only if the two corresponding braid words are equal modulo the following equations:*

$$\mathbb{i} \cdot \mathbb{j} = \mathbb{j} \cdot \mathbb{i} \qquad |\mathbb{i} - \mathbb{j}| > 1 \tag{5.1}$$

$$\mathbb{i} \cdot \mathbb{j} \cdot \mathbb{i} = \mathbb{j} \cdot \mathbb{i} \cdot \mathbb{j} \qquad |\mathbb{i} - \mathbb{j}| = 1 \tag{5.2}$$

The confluence problem of braids is then the question whether we can extend two given braids, such that they become equal. Deciding braid equivalence corresponds to the word problem with respect to the identities 5.1 and 5.2 and is decidable, which is a basic fact, since equations preserve length and, hence, the search space is finite.

Here, we approach the confluence problem for braids via residual systems. In order to show that braids induce a residual system we view braids as reductions. For that crossings are represented as transformations on states. States reflect the relative order of the strands to some initial ordering. For convenience we fix the number of strands in a braid by n. Approaching braids in the context of orthogonality arose from Melliès

[16, 17]. These ideas were factored through the theory of residual system by Klop, van Oostrom & de Vrijer [15]. This is also presented in Terese [23, Chapter 8.9]. The rest of this section is closely oriented on their works.

Definition 5.3.2. The braid abstract rewrite system $\mathcal{B}$ is defined as follows:

- The objects are irreflexive, transitive, and total relations on $\{1, \dots, n\}$ called states.
- The steps are relations, such that for any two states $<, <'$ there exists a step ϕ defined as the relative complement $< - <'$. The src- and tgt-function is then defined by $\mathrm{src}(\phi) := <$ and $\mathrm{tgt}(\phi) := <'$.

We call the steps *braid multi-steps*.

Intuitively speaking a state represents the order of the strands and a multi-step describes the most efficient way to transform one state into another with the least number of crossings. Thus, braid multi-steps represent crossing multiple strands at the same time similar to term rewriting, contracting a number of redex-patterns at the same time. Note that, in particular, no two strands cross twice in a multi-step. Braids are then defined as sequences of multi-steps.

Remark 5.3.3. Since a state $<$ is an irreflexive, transitive, and total relation on $\{1, \dots, n\}$ it imposes a connected strict order, which allows us to abbreviate $<$ by its longest ascending chain in its transitive reduct. For example for $< = \{(1, 2), (1, 3), (2, 3)\}$ it holds that $1 < 2 < 3$ and we hence may abbreviate it by 123. Note that a multi-step is not necessarily total, which is why this abbreviation does not apply.

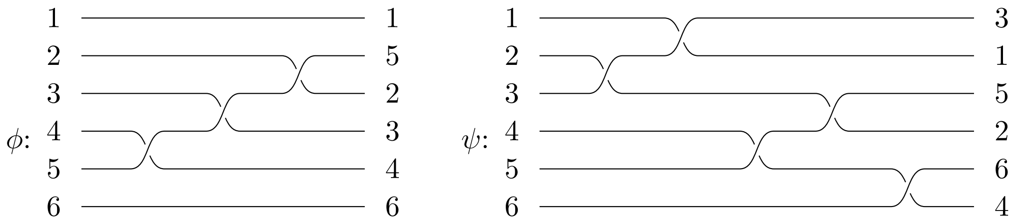
Example 5.3.4. For ϕ, ψ of Figure 5.7a define their source and target as $\mathrm{src}(\phi) := <$, $\mathrm{tgt}(\phi) := <'$, and $\mathrm{src}(\psi) := \ll$, $\mathrm{tgt}(\psi) := \ll'$. By Remark 5.3.3 we abbreviate $< = \ll =$ 123456. Furthermore, $<' = 152346$, $\ll' = 315264$ and $\phi = < - <' = \{(2, 5), (3, 5), (4, 5)\}$, $\psi = \ll - \ll' = \{(1, 3), (2, 3), (2, 5), (4, 5), (4, 6)\}$.

Note the equivalences established in Lemma 3.2.2, which we will use from now on without further reference. The following lemma characterizes braid multi-steps as a scopic and transitive relation.

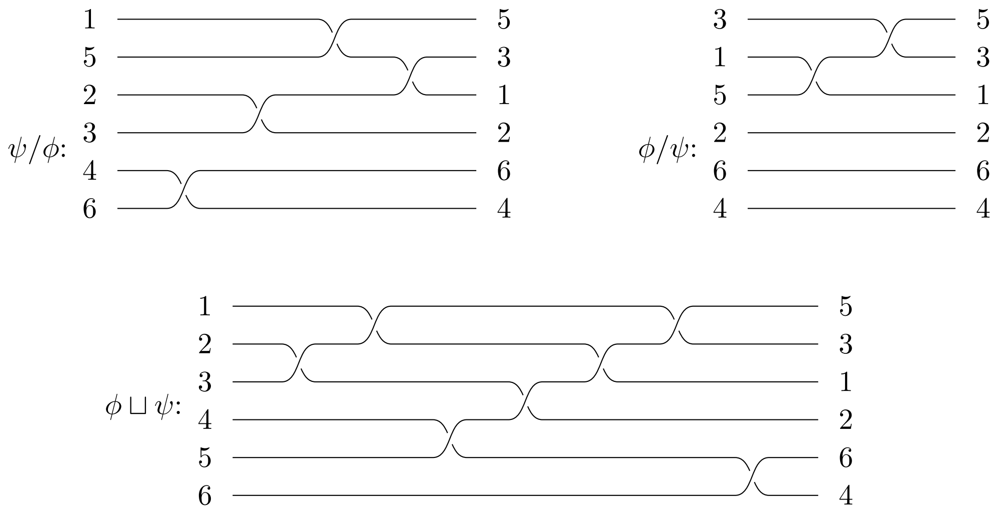
Lemma 5.3.5. *Let $\phi \subseteq <$ for a state $<$. Then, ϕ is a braid multi-step if and only if ϕ is scopic and transitive.*

Proof. (Only-if direction) Let $\phi = < - \ll$. Assume ϕ is not scopic. Then there exists $a < b < c$ with $a \ \phi \ c$ such that $\neg (a \ \phi \ b)$ and $\neg (b \ \phi \ c)$. Hence, $a \ll b \ll c$, which contradicts transitivity of $\ll$ since $(a, c) \in \phi = < - \ll$. Assume ϕ is not transitive, then there exists $a \ \phi \ b \ \phi \ c$ such that $\neg (a \ \phi \ c)$, hence, $a \ (< - \phi) \ c$ by transitivity of $<$, meaning $a \ (< - (< - \ll)) \ c$, which is equal to $a \ (< \cap \ll) \ c$. By totality of $\ll$ it follows that $\neg (c \ll a)$ contradicting transitivity of $\ll$, since $c \ll b \ll a$, which follows again by totality of $\ll$ and $a \ \phi \ b \ \phi \ c$.

(If direction) Let ϕ be scopic and define $\ll := (< - \phi) \cup \phi^{-1} = < + \phi$. Obviously, $\ll$ is irreflexive and total as well. By Lemma 3.2.2 the relation $< - \phi$ is transitive and



(a) Two co-initial braid multi-steps ϕ, ψ defined by $\phi = \{(4,5),(3,5),(2,5)\}$ as well as $\psi = \{(1,3),(2,3),(2,5),(4,5),(4,6)\}$ representing two different transformations of the same state 123456.



(b) The residuals ψ/ϕ and ϕ/ψ as well as the join $\phi \sqcup \psi$ for the co-initial steps ϕ, ψ of Figure 5.7a.

Figure 5.7: Braid multi-steps with their residuals and join.

since ϕ is transitive, too, thus so is ϕ^{-1}. Hence, it remains to show that $(< - \phi) \cdot \phi^{-1}$ respectively $\phi^{-1} \cdot (< - \phi)$ are contained in $\ll$. Therefore, assume $a \; (< - \phi) \; b \; \phi^{-1} \; c$. Since $<$ is irreflexive, transitive and total either $a < c$ or $c < a$.

- $a < c$. Suppose $\neg \, (a \; (< - \phi) \; c)$, then $a \; \phi \; c$ and since $c \; \phi \; b$ with ϕ transitive it follows $a \; \phi \; b$, contradicting the assumption $a \; (< - \phi) \; b$. Consequently $a \ll c$.
- $c < a$. Suppose $\neg \, (a \; \phi^{-1} \; c)$, then also $\neg \, (c \; \phi \; a)$, contradicting the assumption $c < a$. Consequently, $a \ll c$.

Proceed similarly to show $\phi^{-1} \cdot (< - \phi) \subseteq (< - \phi) \cup \phi^{-1}$. Thus, we found a state $\ll$ such that $\phi = < - \ll$ is a multi-step. □

Remark 5.3.6. Note that specifying two components of a multi-step $\phi : < \to \ll$ uniquely determines the third, namely, $\phi = < - \ll$, $< = \ll + \phi^{-1}$ and $\ll = < + \phi$, where addition of sets is done according to Definition 2.1.2. The first characterization is by definition of braid multi-step. For the last one we already saw in the proof of Lemma 5.3.5 that there exists a state $\ll = < + \phi$. Uniqueness follows by the fact that $\ll$ must be the disjoint union of $< - \phi$ and a relation R with $R \cap \phi = \emptyset$. Any such relation R distinct from ϕ^{-1} would violate totality of $\ll$. The second characterization then follows from the third.

We introduce the following definition to state the outcome of a multi-step ϕ on a state $<$, as noted in Remark 5.3.6.

Definition 5.3.7. The *effect* of a multi-step ϕ on the state $<$ is defined as $[\phi] = < + \phi$.

With the effect we can now easily check that dropping one of the two conditions on ϕ stated in Lemma 5.3.5 could result in the target of ϕ not being a state.

Example 5.3.8. Let $< = 123$ and $U = \{(1,2),(2,3)\}$. Note that U and $< + U = \{(1,3),(2,1),(3,2)\}$ are not transitive. Hence, neither is U a multi-step nor is $< + U$ a state. Similarly, for $V = \{(1,3)\}$ the sum is given by $< + V = \{(1,2),(2,3),(3,1)\}$, i.e., V is not scopic and $< + V$ is not transitive.

Intuitively, we can interpret the example above on 123 as follows: On the one hand, swapping 2 and 3 after 1 and 2 have been swapped only works if also 1 and 3 are swapped. On the other hand, 1 and 3 can only cross if either 1 and 2 or 2 and 3 are crossing.

Now, with the fact of a braid multi-step being scopic and transitive in mind, it seems natural to define the join of two multi-steps as the *least* scopic and transitive relation containing both. This is expressed in the following definition (also see Example 5.3.13). That this indeed defines another multi-step is shown in Lemma 5.3.10. Later we will see that this turns out to be the designated join of the to be defined residual system.

Definition 5.3.9. Define for two co-initial steps ϕ, ψ the join $\phi \sqcup \psi$ as the transitive closure of the union of the two steps, i.e.

$$\phi \sqcup \psi := (\phi \cup \psi)^{+}.$$

Lemma 5.3.10. *The join $\phi \sqcup \psi$ of two braid multi-steps ϕ, ψ is again a braid multi-step with src$(\phi \sqcup \psi) =$ src(ϕ).*

Proof. Let $\phi, \psi \subseteq <$ be mutlisteps, i.e. ϕ, ψ are scopic. Since $<$ is transitive and by definition of the closure operator it follows that $(\phi \cup \psi)^+ \subseteq <$. By Theorem 3.2.6 the join is scopic, and therefore with Lemma 5.3.5 also a multi-step. □

On the basis of the join we will define a residuation function for co-initial multi-steps below. Also see Example 5.3.13.

Definition 5.3.11. The residual ψ/ϕ of the co-initial steps ϕ and ψ is defined as the relative complement of ϕ with respect to the join $\phi \sqcup \psi$. Meaning,

$$\psi/\phi := (\phi \sqcup \psi) - \phi.$$

Lemma 5.3.12. *The residual ψ/ϕ of two co-initial braid multi-steps ϕ, ψ is again a braid multi-step with src$(\psi/\phi) = [\phi]$ and tgt$(\psi/\phi) = [\phi \sqcup \psi]$.*

Proof. Let $\mathrm{src}(\phi) = < = \mathrm{src}(\psi)$. Since $<$ is transitive and $\phi, \psi \subseteq <$ it holds that $\phi \sqcup \psi \subseteq <$, and therefore also $(\phi \sqcup \psi) - \phi \subseteq < - \phi$. Thus, $\psi/\phi \subseteq [\phi]$.

We show that $\psi/\phi = [\phi] - [\phi \sqcup \psi]$. Unfolding the effect we have

$$[\phi] - [\phi \sqcup \psi] = ((< - \phi) \cup \phi^{-1}) - ((< -(\phi \sqcup \psi)) \cup (\phi \sqcup \psi)^{-1}).$$

Since $C - (A \cup B) = (C - A) \cap (C - B)$ the set difference can be rewritten into an intersection

$$[\phi] - [\phi \sqcup \psi] = (((< - \phi) \cup \phi^{-1}) - (< - (\phi \sqcup \psi))) \cap (((< - \phi) \cup \phi^{-1}) - (\phi \sqcup \psi)^{-1})$$

with the left part of the intersection equal to $(((\phi \sqcup \psi) - \phi) \cup \phi^{-1})$, since $\phi \subseteq \phi \sqcup \psi$ as well as $\phi^{-1} \not\subseteq \phi \sqcup \psi$, and with the right part equal to $< - \phi$. Hence, the difference of the effects simplifies to $[\phi] - [\phi \sqcup \psi] = (\phi \sqcup \psi) - \phi$ proving that ψ/ϕ is a step from $[\phi]$ to $[\phi \sqcup \psi]$. □

Example 5.3.13. Consider ϕ and ψ of Figure 5.7a. Then

$$\phi \sqcup \psi = \{(1,3), (1,5), (2,3), (2,5), (3,5), (4,5), (4,6)\}.$$

Hence, $\psi/\phi = \{(1,3), (1,5), (2,3), (4,6)\}$, $\phi/\psi = \{(1,5), (3,5)\}$, compare Figure 5.7b.

Remark 5.3.14. Comparing Figure 5.7a and 5.7b we see that ϕ is composable with ψ/ϕ at state 152346 (similarly ψ with ϕ/ψ) and indeed ψ/ϕ and ϕ/ψ are co-final with $\mathrm{tgt}(\psi/\phi) = 531264 = \mathrm{tgt}(\phi/\psi)$, already suggesting what we will show in Theorem 5.3.16, namely, that / actually is a residuation for a residual system for braids.

Remark 5.3.15. One may further notice, that $\mathrm{tgt}(\phi \sqcup \psi)$ also equals 531264, i.e., $\phi \sqcup \psi$ is co-final with ψ/ϕ and ϕ/ψ (see Figure 5.7b). As we will see later this is no coincidence, since the join $\sqcup$ will turn out to be the designated binary join of the residual system mentioned in Remark 5.3.14.

Theorem 5.3.16. *$\langle \mathcal{B}, \emptyset, / \rangle$ is a residual system.*[3]

Proof. That / is a residuation for braid multi-steps was shown in Lemma 5.3.12. The laws R2–R4 are obvious by transitivity of multi-steps. Only the cube law R1 is non-trivial.

Let ϕ, ψ, χ be braid multi-steps from $<$. By definition

$$\begin{aligned}(\phi/\psi)/(\chi/\psi) &= ((\chi/\psi) \sqcup (\phi/\psi)) - (\chi/\psi) \\ &= (((\psi \sqcup \chi) - \psi) \cup ((\psi \sqcup \phi) - \psi))^+ - (\chi/\psi) \\ &= (((\psi \sqcup \chi) \cup (\psi \sqcup \phi)) - \psi)^+ - (\chi/\psi)\end{aligned}$$

Since $\psi \subseteq (\psi \sqcup \chi) \cap (\psi \sqcup \phi)$ Lemma 2.1.10 applies and we can simplify accordingly.

$$\begin{aligned}(\phi/\psi)/(\chi/\psi) &= (((\psi \sqcup \chi) \cup (\psi \sqcup \phi))^+ - \psi) - ((\psi \sqcup \chi) - \psi) \\ &= (((\psi \sqcup \chi) \cup (\psi \sqcup \phi))^+ - \psi) - (\psi \sqcup \chi) \\ &= ((\psi \sqcup \chi) \cup (\psi \sqcup \phi))^+ - (\psi \sqcup \chi) \\ &= ((\psi \sqcup \chi) \sqcup \phi) - (\psi \sqcup \chi) \\ &= \phi/(\psi \sqcup \chi)\end{aligned}$$

where we made multiple use of Lemma 2.1.11 for the fourth equality. Concluding, $(\phi/\psi)/(\chi/\psi) = \phi/(\psi \sqcup \chi) = \phi/(\chi \sqcup \psi) = (\phi/\chi)/(\psi/\chi)$ by commutativity of the join, which proves the claim. □

Lemma 5.3.17. *The function $\sqcup$ for braid multi-steps is the designated join for the residual system $\langle \mathcal{B}, \emptyset, / \rangle$.*

Proof. From $\phi \cdot (\psi/\phi) = \phi \cdot ((\phi \sqcup \psi) - \phi) \subseteq \phi \sqcup \psi$ we can directly infer that $(\phi \cdot (\psi/\phi))/(\phi \sqcup \psi) = \emptyset$ holds. Hence, $\phi \cdot (\psi/\phi) \lesssim \phi \sqcup \psi$. That also $\phi \sqcup \psi \lesssim \phi \cdot (\psi/\phi)$ follows from C2, the fact that $\phi \sqcup \psi \sqcup \phi = \phi \sqcup \psi$, and R2. □

That the braid abstract rewrite system is confluent follows immediately from the residuation function. To see that braids are also confluent we simply develop a braid multi-step into a series of crossings. This can be done by selecting a pair of crossing strands from the multi-step and perform the crossing. Then, repeat on the residual of the multi-step after the crossing. This procedure is terminating, since the size of the multi-step strictly decreases with each crossing. With the residuation satisfying the residual identities R1–R4 it yields the least direct continuation of two co-initial braids, such that they become equal under Artin's positive braid relations.

[3] $\emptyset$ denotes the empty relation acting as a unit for any state.

6 Self-Distributivity

This chapter is solely dedicated to orthogonality of self-distributivity by constructing a residual system. Its presentation shows resemblance to that of braids. One problem deriving a skolem function for the diamond property of many-steps satisfying the residual identities is rooted in the infinite behaviour caused by created redexes. We deal with these created redexes by means of tracing and developments similar to the case of associativity. Termination of these developments will be shown via a normalizing strategy, bearing resemblance to the S-combinator considering an inductive definition as a normalizing, innermost strategy.

A binary operation is self-distributive if either the equality $(a * b) * c = (a * c) * (b * c)$ or the equality $a * (b * c) = (a * b) * (a * c)$ holds. In the former case it is called right self-distributive and in the latter case left self-distributive. As the properties of both equalities are symmetric we will investigate only the former. The first section provides a collection of selected models of self-distributivity. In the second section we turn the equational system into a rewrite system in the length increasing direction and enrich the TRS by further steps defined via developments. With local confluence we also show the first result on developments. The third section deals with the termination of developments via an optimal strategy. The last section then derives a residual system for self-distributivity.

6.1 Exemplifying Models for Self-Distributivity

Simple examples of self-distributive operations are the logical $\wedge$ and $\vee$, since they are associative, commutative and idempotent, which verifies the following:

$$(x \wedge y) \wedge z = (x \wedge z) \wedge (y \wedge z)$$
$$(x \vee y) \vee z = (x \vee z) \vee (y \vee z)$$

The geometrical example of middle provides a quite illustrative model in any higher-dimensional space.

Example 6.1.1. *(Geometrical middle)* Define for $a, b \in \mathbb{R}^n$ the operation $*$ as a binary function over the n-dimensional space mapping a, b to the midpoint between a and b, i.e.,

$$a * b := a + \tfrac{1}{2}(b - a).$$

Then the operation $*$ is self-distributive, see Figure 6.1, as

$$(a * b) * c = \tfrac{1}{4}a + \tfrac{1}{4}b + \tfrac{1}{2}c = (a * c) * (b * c).$$

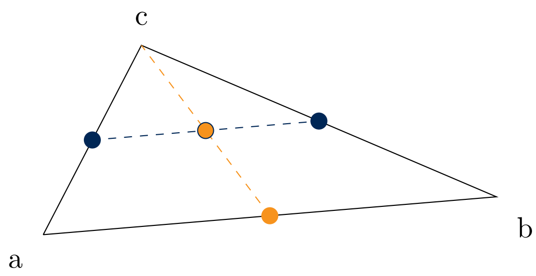


Figure 6.1: Geometric interpretation of middle in $\mathbb{R}^n$. Orange corresponds to $(a * b) * c$ and blue to $(a * c) * (b * c)$.

In topology quandles are defined via self-distributivity. We will not recapitulate the study of quandles here but only give an example representing quandles of a very specific form to give an idea to the reader.

Example 6.1.2. *(Conjugation quandle)* Let G be a group. Define for $a, b \in G$ the operation $*$ by

$$a * b := b^{-1}ab.$$

Then, as the operation $*$ is idempotent, it also is self-distributive, namely

$$(a * b) * c = c^{-1}b^{-1}abc = (a * c) * (b * c).$$

The interested reader may study Dehornoy's overview on the *world* of self-distributivity, which offers a great collection of various other models from topology [9].

Another model involves braids of Section 5.3. It goes back to Dehornoy's construction of his *Blueprint* of a term [8] and shows similarities to the conjugation quandle. The operation is defined on two braids with infinitely many strands.

Example 6.1.3. *(Shifted braid conjugation with one added crossing)* Let a, b be two braid words of braids with positive and negative crossings on infinitely many strands. Inductively define by $\mathrm{sh}(\epsilon) = \epsilon$, $\mathrm{sh}(\mathbb{i} \cdot a) = (\mathbb{i} + \mathbb{1}) \cdot \mathrm{sh}(a)$ a shift of the whole braid by one strand. Furthermore, define

$$a * b := \mathrm{sh}(b)^{-1} \cdot \mathbb{1} \cdot \mathrm{sh}(a) \cdot b.$$

Consequently, the following identity holds due to Artin's first braid equivalence (5.1):

$$(a * b) * c = \mathrm{sh}(c)^{-1} \cdot \mathrm{sh}(\mathrm{sh}(b))^{-1} \cdot \mathbb{1} \cdot \mathbb{2} \cdot \mathrm{sh}(\mathrm{sh}(a)) \cdot \mathrm{sh}(b) \cdot c = (a * c) * (b * c),$$

meaning $*$ is self-distributive. Here we made implicit use of the notational convention of $(\mathrm{w}w)^{-1} = w^{-1}\mathrm{w}^{-1}$ and $\epsilon^{-1} = \epsilon$ for a word w, the empty word ϵ and an element w. Obviously, a crossing followed by its inverse crossing is the empty crossing, i.e., $\mathbb{i} \cdot \mathbb{i}^{-1} = \epsilon$.

Our last interpretation concerns substitution of the well-known λ-calculus and requires some more background, which will only be provided very briefly. The Substitution Lemma, which the following example depends on, can be found in the comprehensive monograph by Barendregt [3, Lemma 2.1.10] and in Terese [23, Lemma 10.1.10]. Both works provide further details and facts on λ-calculus.

Example 6.1.4. *(Substitution of λ-calculus)* The λ-calculus considers the calculus of λ-terms defined by the grammar

$$t ::= x \mid (t\,t) \mid (\lambda x.t)\ ,$$

where x is from an infinite set $\mathcal{V}$ of variables. The second clause is called application and the third clause is called abstraction. Application associates to the left. Moreover, for abstractions the scope is extended to the right as far as possible. An occurrence of x in $\lambda x.t$ is called bound, otherwise it is called free. By $t \equiv s$ it is denoted that t and s are identical terms or t can be obtained from s by renaming bound variables without variable capture, i.e., $\lambda x.x\,z \equiv \lambda y.y\,z \not\equiv \lambda z.z\,z$.

The substitution of the free occurrence of x in s by t, written as $s[x := t]$ is then inductively defined by

$$\begin{aligned} x[x := t] &\equiv t \\ y[x := t] &\equiv y \\ (s_1\,s_2)[x := t] &\equiv (s_1[x := t])\,(s_2[x := t]) \\ (\lambda y.s)[x := t] &\equiv \lambda y.(s[x := t]). \end{aligned}$$

To avoid that free variables become bound after substitution in expressions like $M[x := N]$ we assume that variables occurring free in N do not become bound after substitution in the term M, and that the substitution variable x does not occur bound in M. One way of achieving this is by suitable renaming of variables.

The following lemma is a well-known result and provides the claim of substitution being self-distributive.

Substitution Lemma. Let s, t, u be λ-terms. It holds that

$$s[y := t][z := u] \equiv s[z := u][y := t[z := u]],$$

if y is not a free variable in u and $y \not\equiv z$.

A proof of the lemma uses structural induction over λ-terms and can be found in referred literature. The substitution lemma is the key property in Tait and Martin-Löf's confluence proof of β-reductions via the diamond property of parallel β-reductions refined by Takahashi [22].

6.2 Treks and Developments

After a collection of self-distributive models we now take a rewriting perspective on self-distributivity. The system obtained from the rule in length decreasing direction is obviously terminating. However, as far as the author is aware all completion tools fail on that system. Hence, we consider the system in length increasing direction, which is not terminating. After its introduction we will enrich the system by further steps via developments of to be defined treks. The naming goes back to Melliès [16]. Basically, a trek can be seen as a development, where not all 'elements' are redexes yet, however, the 'elements' can be seen as virtual redexes as they develop into redexes along a development of the trek. Showing that these developments indeed uniquely define steps, i.e., a complete development results in a unique target is the goal of the next section. Here we will only see a first step into that direction, namely that developments of treks are locally-confluent.

The term rewriting system of self-distributivity $\mathcal{T}_{SD}$ consists of the signature Σ_{SD} over a single binary function symbol $*$ and a rule set $R_{SD} := \{\rho : (x*y)*z \to (x*z)*(y*z)\}$. We adopt notation from Chapter 5 and may use $*$ in implicit infix notation, while associating to the left, thus we write

$$\rho : xyz \to xz(yz).$$

A proof term defining a single-step over $\mathcal{T}_{SD}$ will also be called an SD-step. That SD-steps do not have the diamond property can easily be inferred from Figure 6.4 on page 61.

Note that the redex-pattern (see Definition 5.2.9) of a single SD-step ϕ consists of a pair, i.e., $\mathcal{RPos}(\phi) = \{\alpha, \alpha 0\}$ for some $\alpha \in \mathcal{Pos}$. Hence, for a given term t we can characterize a single SD-step by an ordered pair of the form $(\alpha, \alpha 0)$ or even simply by α and mean the proof term ϕ with the source t and $\rho \in R_{SD}$ at position α. We will use all three characterizations interchangeably, if they are evident from the context. Based on that observation we define the SD-pairs of a parallel SD-step.

Definition 6.2.1. Let ϕ be a single SD-step. The redex pair $\mathcal{RPair}(\phi)$ of ϕ is the ordered pair defined by

$$\mathcal{RPair}(\phi) = (\alpha, \alpha 0) \text{ such that } \{\alpha, \alpha 0\} = \mathcal{RPos}(\phi).$$

Example 6.2.2. Let $\phi = \rho(*(w, x), y, z) : wxyz \to_{SD} wxz(yz)$ and $\psi = *(\rho(w, x, y), z) : wxyz \to_{SD} wy(xy)z$. Then, $\mathcal{RPair}(\phi) = (\epsilon, 0)$ and $\mathcal{RPair}(\psi) = (0, 00)$.

Hence, we can represent an SD-step from a given term by an ordered pair. The first entry describes the position of the redex. The second element might seem superfluous, but it will allow us to consider the transitive closure analogue to braid multi-steps. Next we define the notion of a trek, which is a pair consisting of a term and a set of ordered position pairs under certain restrictions. Note that in the following we interpret a term as a strict prefix order (see Definition 2.1.7) of its non-variable positions, e.g., the term $t = a * (b * c) * d$ is interpreted as a set of position pairs defined as follows $\{(\epsilon, 0), (\epsilon, 01), (0, 01)\}$.

Definition 6.2.3. A *trek* (t, U) consists of a term t (interpreted as the strict prefix order of its non-variable positions) and a binary relation U satisfying

SD1 $U \subseteq t$

SD2 U is transitive

SD3 U is scopic in t

SD4 $\forall(\alpha, \beta\gamma) \in U : \alpha = \beta \implies 0 \sqsubseteq \gamma$

Intuitively, a trek can be interpreted as a collection of tasks U that are to be performed in a term t. Each pair is one task. However, to be able to perform a task the pair needs to have the form $(\alpha, \alpha 0)$ for some $\alpha \in \mathcal{P}os$, which we then call a single SD-step α. Here we can think of terms as states in the braid case, where positions additionally carry a history. The history keeps track of the current element and which elements were originally greater than the current element. The history of a position is carried in its right sub-term. The left-most element of that right sub-term is the current element at that position, i.e., a position is represented by the left-most variable of its right sub-term. This intuition factors through the whole term tree inductively. Then, a task is to swap right sub-terms at the two positions of a task's pair, i.e., we want to swap elements including history. The following example illustrates the procedure, which will be formalized with *developments* later.

Example 6.2.4. Consider xyz. In the braid case we would read it as the state $x < y < z$, in the SD case we read it as the term $x * y * z$. Call this term t and let $U = \{(\epsilon, 0)\}$, then (t, U) defines a trek, since U satisfies SD1–SD4. Note that U^{-1} also defines a braid multi-step when interpreting it as $\{(y, z)\}$. Performing the corresponding step

$$x\ \overset{\curvearrowleft}{yz}$$

results in $x < z < y$ in the braid case. We could read it as *x is smaller z is smaller y*. According to self-distributivity the trek (t, U) should result in $x * z * (y * z)$. We could read it as *x is smaller z is smaller y, which was smaller z*, i.e., a braid with memory.

So SD1–SD3 can be interpreted in the same way as for braid multi-steps. Additionally, SD4 prevents that elements in the history are swapped with the original element. Note, that we interpret t as the prefix order of its position, meaning we only swap from right to left. Also we assumed that we started with a linear term. However, several problems arise. First, it is not evident that each non-empty trek contains a pair of sub-terms that can be swapped, i.e., a pair of adjacent positions. Second, performing a swap should result in a trek again. Third, as histories may become duplicated one problem is the question whether repeated swapping terminates.

Concerning the first problem we show as an intermediate result that between any two positions of a pair contained in a trek there exists a step.

Lemma 6.2.5. *Let (t, U) be a trek, such that $(\alpha, \beta) \in U$ then there exists $(\gamma, \gamma 0) \in U$ with $\alpha \sqsubseteq \gamma \sqsubset \gamma 0 \sqsubseteq \beta$.*

Proof. We show the claim by induction over the distance (see Definition 2.1.3) d from α to β. Let $n = 1$. Due to SD4 $\beta = \alpha 0$, hence, there is nothing to show. If $n > 1$ there exists $\delta \in \mathcal{P}os_{\Sigma}(t)$ with $\alpha \sqsubset \delta \sqsubset \beta$. Since t is transitive and U is scopic with respect to t, it follows by Lemma 3.2.2 that $\alpha\ U\ \delta \vee \delta\ U\ \beta$. By induction hypothesis the statement holds on the former or the latter case. □

Now, it is easy to derive the existence of a redex-pair in any trek (t, U) with U non-empty.

Corollary 6.2.6. *If (t, U) is a trek and U is non-empty, then $(\gamma, \gamma 0) \in U$ for some $\gamma \in \mathcal{P}os_{\Sigma}(t)$.*

Proof. Since U is non-empty, choose $(\alpha, \beta) \in U$. Then, the corollary is a direct consequence of Lemma 6.2.5. □

Hence, by above corollary every non-empty trek contains a step. However, the question whether swapping a pair, i.e., performing a step, results in a trek again and the question whether swapping terminates haven't been answered yet. We approach the former problem by tracing, drawing a parallelism to associativity of Section 5.2. The latter problem we approach similar to the S-rule in Section 5.1, where we were also facing a termination issue, which was rooted in duplication. We handled this issue by defining the residuation recursively. Considering a recursive definition as a normalizing strategy for their evaluation, namely the innermost strategy, we will proceed analogue for self-distributivity. However, for the self-distributive case we will not use a recursive definition, but directly formulate a normalizing strategy.

Let us turn our attention to the first remaining question. For associativity we defined a bijective rule tracing. This is not possible for self-distributivity, since the rule ρ is length increasing. Nonetheless, another quite natural rule tracing exists, which fits our intuition that non-variable positions are represented by the left-most variable of its right sub-term. According to this intuition the position 0 of the left-hand side xyz represents y and the position ϵ of the right-hand side $xz(yz)$ also represents y. Hence, it seems reasonable to trace 0 to ϵ. Proceeding similar for the position ϵ in the term xyz is a bit more complex as it represents the variable z, which is represented by two positions in the right-hand side, namely 0 and 1. But this simply suggests to trace ϵ to both 0 and 1. By definition of rule tracing we trace variable positions to the corresponding variable positions in the right-hand side. Thus, define the rule tracing of the rule ρ by

$$[\rho\rangle = \{(\epsilon, 0), (\epsilon, 1), (0, \epsilon), (00, 00), (01, 10), (1, 01), (1, 11)\}$$

(see Figure 6.2). However, we do not only want to trace terms along steps but we also want to trace the position pairs U of a trek (t, U). These position pairs represent the variables that we want to swap including their history. As we consider U as a subset of the non-variable positions of t, i.e., $U \subseteq t$, we are only interested in those traced pairs that belong to the traced term. This is done by first pointwise tracing analogously to what we have done before. However, we then only consider those pairs that belong to the strict prefix order.

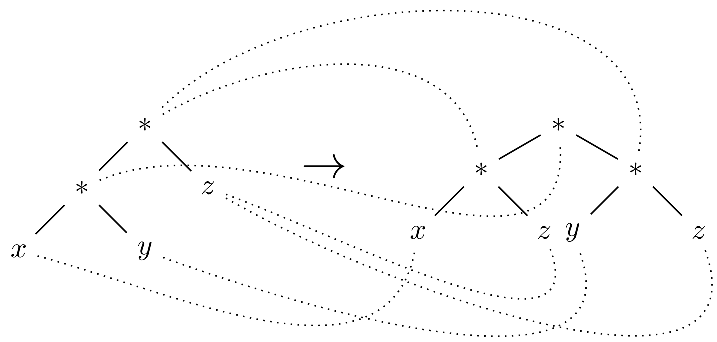


Figure 6.2: Source and target of a single SD-step ρ as term trees and the corresponding rule tracing $[\rho\rangle$ indicated by dotted lines.

Definition 6.2.7. For a proof term ϕ we define the *strict prefix* trace of a binary relation $U \subseteq \mathcal{P}os \times \mathcal{P}os$ by

$$U_{[[\phi\rangle\rangle} := (U[[\phi\rangle\rangle) \cap \sqsubset .$$

Strict prefix trace is abbreviated by sp-trace.

Formally defining the procedure of repeated swapping via treks requires that swapping sub-terms in t according to a redex-pair in U results in a trek again, i.e., for a trek (t, U) performing a single-step α contained in U as $(\alpha, \alpha 0) \in U$ results in a trek. This is proven formally in the next lemma.

Lemma 6.2.8. *Let (s, U) be a trek and let $\phi : s \to_{SD} t$ be a single SD-step with $\mathcal{RP}air(\phi) \in U$, then $(t, U_{[[\phi\rangle\rangle})$ is a trek as well.*

Proof. SD1: Let $(\alpha, \beta) \in U \subseteq \mathcal{P}os_\Sigma(s)$, then by definition of the trace relation $(\alpha[[\phi\rangle\rangle), (\beta[[\phi\rangle\rangle) \subseteq \mathcal{P}os_\Sigma(t)$. Hence, $(U[[\phi\rangle\rangle) \subseteq \mathcal{P}os_\Sigma(t) \times \mathcal{P}os_\Sigma(t)$. Intersecting both sides of the inclusion with the strict prefix relation $\sqsubset$ proves that $U_{[[\phi\rangle\rangle} \subseteq t$.

SD2: First note that for each $\alpha' \in \mathcal{P}os(t)$ there exists exactly one $\alpha \in \mathcal{P}os(s)$, such that $\alpha\ [[\phi\rangle\rangle\ \alpha'$. This is due to the inverse of the rule tracing $[\rho\rangle^{-1}$ being a function and due to the rule ρ being left-linear. Similarly define for $\beta', \gamma' \in \mathcal{P}os(t)$ the position $\beta, \gamma \in \mathcal{P}os(s)$, such that $\beta\ [[\phi\rangle\rangle\ \beta'$ and $\gamma\ [[\phi\rangle\rangle\ \gamma'$. Assume $\alpha'\ U_{[[\phi\rangle\rangle}\ \beta'\ U_{[[\phi\rangle\rangle}\ \gamma'$, then $\alpha\ U\ \beta\ U\ \gamma$. By transitivity of U also $\alpha\ U\ \gamma$, hence, by transitivity of $\sqsubset$ it follows that $\alpha'\ U_{[[\phi\rangle\rangle}\ \gamma'$.

SD3: As above, define for $\alpha', \beta', \gamma' \in \mathcal{P}os(t)$ the unique elements in the domain of $[[\phi\rangle\rangle$ relating to them by $\alpha, \beta, \gamma \in \mathcal{P}os(s)$. Assume $\alpha' \sqsubset \beta' \sqsubset \gamma'$ and $\alpha'\ U_{[[\phi\rangle\rangle}\ \gamma'$. Then, by definition of the trace relation $[[\phi\rangle\rangle$ also $\alpha\ U\ \gamma$. If $\alpha \sqsubset \beta \sqsubset \gamma$ it follows by scopicness of U that $\alpha\ U\ \beta \vee \beta\ U\ \gamma$, which implies $\alpha'\ U_{[[\phi\rangle\rangle}\ \beta' \vee \beta'\ U_{[[\phi\rangle\rangle}\ \gamma'$. If $\alpha \sqsubset \beta \sqsubset \gamma$ does not hold, either $\beta \sqsubset \alpha \sqsubset \gamma$ or $\alpha \sqsubset \gamma \sqsubset \beta$, since a single-step preserves the prefix relation of position pairs except for $\mathcal{RP}air(\phi)$. Hence, in the former case $\mathcal{RP}air(\phi) = (\beta, \alpha)$, i.e., $\beta\ U\ \alpha\ U\ \gamma$ and by transitivity of U it holds that $\beta\ U\ \gamma$, which implies $\beta'\ U_{[[\phi\rangle\rangle}\ \gamma'$. Correspondingly, the latter case implies $\alpha'\ U_{[[\phi\rangle\rangle}\ \beta'$. So, $U_{[[\phi\rangle\rangle}$ is scopic in t.

SD4: Assume $\alpha'\ U_{[[\phi\rangle\rangle}\ \alpha'\gamma'$, then by definition of $[[\phi\rangle\rangle$ there exist unique $\alpha, \delta \in \mathcal{P}os(s)$ with $\alpha\ [[\phi\rangle\rangle\ \alpha'$ and $\delta\ [[\phi\rangle\rangle\ \alpha'\gamma'$ such that $\alpha\ U\ \delta$. Since $U \subseteq \sqsubset$ there exists $\gamma \in \mathcal{P}os$, such that $\delta = \alpha\gamma$. Since (s, U) is a trek, it holds that $0 \sqsubseteq \gamma$. Let $C[\ ]$ be a context, such that $\phi = C[\rho(x^\sigma, y^\sigma, z^\sigma)]$ for some substitution σ. We proceed by a case distinction on the relative positions of α, γ with respect to the step ϕ. If $\alpha, \alpha\gamma$ are non-hole positions in the context $C[\ ]$ it holds that $\alpha' = \alpha$ and $\gamma' = \gamma$, hence, $0 \sqsubseteq \gamma'$. If only α is a non-hole position in $C[\ ]$ either $\alpha\gamma$ is the position of the hole or $\alpha\gamma$ is a position in the ρ-redex. Either way, the position of the ρ-redex is in the left sub-term of α, which also holds for the target of ϕ, thus, on the one hand $\alpha' = \alpha$ and on the other hand $0 \sqsubseteq \gamma$ implies $0 \sqsubseteq \gamma'$. If α is the position of the hole in $C[\ ]$, i.e., the position of the ρ-redex, $\alpha\gamma$ is in either the first or the second argument of ρ. This is due to (s, U) being a trek, SD4 to be precise, and the fact that $\gamma \neq 0$ by the definition of $[\rho\rangle$. Hence, $\alpha' = \alpha 0$ in the first-argument-case, $\alpha' = \alpha 1$ in the second-argument-case and $0 \sqsubseteq \gamma'$ in both cases (see Figure 6.2). If α and $\alpha\gamma$ are no positions in $C[\ ]$, the trace preserves γ, i.e., $\gamma' = \gamma$, with the only exception when α is the position of the sub-term $x^\sigma * y^\sigma$, where $\gamma' = 0\gamma$. Nonetheless, it holds that $0 \sqsubseteq \gamma'$. □

With developments we now formalize the procedure of repeated swapping. Basically, a development of a trek (s, U) takes a redex-pair from U, which was shown to exist, and applies the corresponding step to s. The relation U is traced accordingly and the procedure possibly repeated. If the procedure cannot be repeated any further, we call the development complete.

Definition 6.2.9. A *development* of a trek (s, U) is co-inductively defined as either the empty step 1 or a single SD-step $\phi : s \to_{SD} t$, such that $\mathcal{RP}air(\phi) \in U$, composed with a development of $(t, U_{[[\phi\rangle\rangle})$. A development is *complete*, if it cannot be extended any further.

Remark 6.2.10. Like developments in the case of associativity, here, the definition of development of a trek is also co-inductive, i.e., infinite sequences are not excluded. Well-definedness follows by the fact that $s\ [[\phi\rangle\rangle\ t$ for $\phi : s \to t$. Lemma 6.2.8 ensures that the trace of a trek (s, U) is a trek again, namely $(t, U_{[[\phi\rangle\rangle})$. Corollary 6.2.6 ensures that there always exists a step in $U \neq \emptyset$. Hence a development is complete, if $U = \emptyset$.

Example 6.2.11. There exist two complete developments of the following trek:

$$(wxyz, \{(\epsilon, 0), (\epsilon, 00), (0, 00)\}).$$

See Figure 6.4.

One of the greatest benefits arising from the definition of trek is that they do not terminate before they are complete. Differently speaking, they do not get stuck. For that reason all effort for the definition of trek went into making the above example *work*, i.e., making both developments terminate in $(wz(yz)(xz(yz)), \emptyset)$. Hence, in the same way

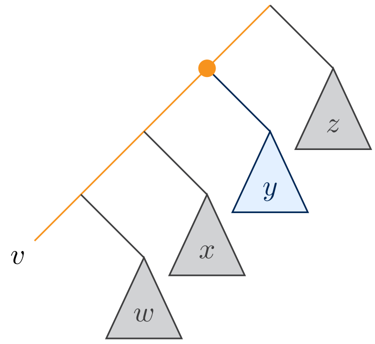


Figure 6.3: Visualizing the condition of SD4. A vertebra (orange dot) on the spine (orange edges) cannot be swapped with a position of its right sub-term (blue).

as scopic relations were needed to describe a transitive relation as a braid multi-step here SD4 is needed to interpret a braid multi-step as a trek. To sharpen the intuition we can think of the positions consisting only of zeros as the vertebrae on the spine of the leftmost variable of the term t. In the analogy of swapping sub-terms SD4 prevents any vertebra on the spine to be swapped with any position in its sub-term on the right (see Figure 6.3).

With the next theorem we prove the first step into the direction of confluence and termination of treks.

Theorem 6.2.12. *Treks are locally confluent.*

Proof. We show that for two single SD-steps $\phi : s \to_{SD} t_1$ and $\psi : s \to_{SD} t_2$ with $\mathcal{RP}air(\phi), \mathcal{RP}air(\psi) \in U$ we find a common reduct for $(t_1, U_{[[\phi\rangle\rangle})$ and $(t_2, U_{[[\psi\rangle\rangle})$.

Let $\phi = C[\rho(x^\sigma, y^\sigma, z^\sigma)], \psi = D[\rho(x^\tau, y^\tau, z^\tau)]$ and let the hole in $C[\,]$ be at position α and the hole in $D[\,]$ be at position β. Then $\mathcal{RP}air(\phi) = (\alpha, \alpha 0)$ and $\mathcal{RP}air(\psi) = (\beta, \beta 0)$. We distinguish between orthogonal and non-orthogonal steps as of Section 4.2, i.e., between $\phi \perp \psi$ and $\phi \not\perp \psi$.

Finding co-final proof terms in the former case is trivial, as we can simply trace the redex-pair of the other, as ϕ and ψ do not overlap, since the trace relation is based on $[\rho\rangle$ in a parametric way, i.e., a redex-pair traces to redex-pairs again.

In the latter case there exist two rule-based function symbol occurrences in s with respect to ϕ, namely $\langle * \mid C[\,]\rangle$ and $\langle * \mid C[*(\Box, s')]\rangle$ for some term s'. Since $[[\phi\rangle\rangle$ is parametric we can assume without loss of generality that $C[\,] = \Box$. Then the second function symbol occurrence is also rule-based with respect to ψ and we have $\phi = \{(\epsilon, 0)\}, \psi = \{(0, 00)\}$. By transitivity of U it follows that $(\epsilon, 00) \in U$. Hence, $\{(0, 00)\} \cdot \{(\epsilon, 0)\} : t_1 \to t$ and $\{(\epsilon, 0)\} \cdot \{(0, 00), (1, 10)\} : t_2 \to t$ (see Figure 6.4). The equality $(U[[\{(\epsilon, 0)\} \cdot \{(0, 00)\} \cdot \{(\epsilon, 0)\}\rangle\rangle) = (U[[\{(0, 00)\} \cdot \{(\epsilon, 0)\} \cdot \{(0, 00), (1, 10)\}\rangle\rangle)$ holds, since we trace position pairs of the term s along either co-final composition path. Consequently $U_{[[\{(\epsilon,0)\}\cdot\{(0,00)\}\cdot\{(\epsilon,0)\}\rangle\rangle} = U_{[[\{(0,00)\}\cdot\{(\epsilon,0)\}\cdot\{(0,00),(1,10)\}\rangle\rangle}$ and (s, U) is locally confluent. $\Box$

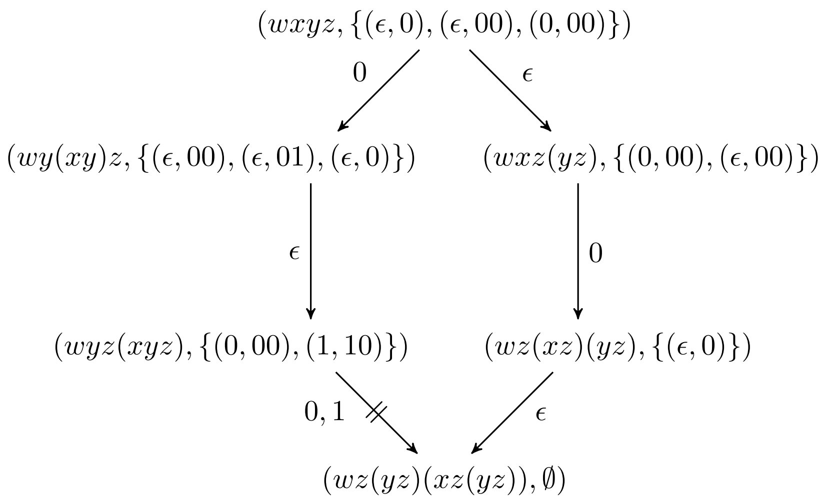


Figure 6.4: Two complete developments of the trek $(wxyz, \{(\epsilon, 0), (\epsilon, 00), (0, 00)\})$.

6.3 Completeness of Developments

After we saw that treks are locally confluent we now aim to show termination of treks to be able to apply Newman's Lemma. To do so, we define a well-order on trees and derive a terminating strategy according to that order for developing treks.

Definition 6.3.1. Define $<_{\text{rev}}$ as the *reversed in-order tree traversal*, i.e., as the relation on positions of a term $t = C[t_0 \cdot t_1]$, such that $p1p_1 <_{\text{rev}} p <_{\text{rev}} p0p_0$, where p is the position of the hole in $C[\ ]$ and $p_0 \in \mathcal{P}os(t_0), p_1 \in \mathcal{P}os(t_1)$.

Lemma 6.3.2. *The relation $<_{rev}$ is a well-order.*

Proof. Since the in-order tree traversal visits each node of a tree exactly once, and since we recursively order the positions by the visit of the corresponding node, $<_{\text{rev}}$ is transitive, anti-symmetric, and total. ☐

Definition 6.3.3. Let $\to_{\text{rev}}$ be the strategy, that for a trek (t, U) applies the smallest step $(\alpha, \alpha 0) \in U$ according to reversed in-order tree traversal.

Remark 6.3.4. The ARS $\to_{\text{rev}}$ is indeed a strategy for developing treks, since the objects of $\to_{\text{rev}}$ are also treks and the normal forms of $\to_{\text{rev}}$ are exactly the treks of the form $(t, \emptyset)$, i.e., equal to the normal forms of developments. Furthermore, the strategy $\to_{\text{rev}}$ is deterministic, since $\to_{\text{rev}}$ is a well-order.

Next, we will state some observations we will be using later. The first observation is, that whenever we apply a step $(\gamma, \gamma 0) \in U$ according to $\to_{\text{rev}}$ there exists no position pair in U with a second component above γ.

Lemma 6.3.5. *Let (t, U) be a trek and let $(\gamma, \gamma 0) \in U$ be minimal according to $<_{rev}$ among all possible steps in U. Then, for all $(\alpha, \beta) \in U$ it holds, that $\gamma \sqsubseteq \beta$ or $\alpha \parallel \gamma$.*

Proof. Assume there exists a pair $(\alpha, \beta) \in U$, such that $\gamma \sqsubseteq \beta \vee \alpha \parallel \gamma$ does not hold. Since $\alpha \sqsubset \beta$ this implies $\beta \not\parallel \gamma$, i.e., $\beta \sqsubset \gamma$. By Lemma 6.2.5 there exists $(\delta, \delta 0) \in U$ with $\alpha \sqsubseteq \delta \sqsubset \delta 0 \sqsubseteq \beta$ contradicting minimality of γ according to $<_{\text{rev}}$. □

We can even narrow the previous lemma down to a stronger statement about the second components of position pairs. Namely, there furthermore exists no position pair with a second component in the right sub-term of γ.

Lemma 6.3.6. *Let (t, U) be a trek and let $(\gamma, \gamma 0) \in U$ be minimal according to $<_{rev}$ among all possible steps in U. Then, for all $(\alpha, \beta) \in U$ it holds, that $\gamma 0 \sqsubseteq \beta$ or $\alpha \parallel \gamma$.*

Proof. Assume $\gamma 0 \not\sqsubseteq \beta \wedge \alpha \not\parallel \gamma$. By Lemma 6.3.5 it holds that $\gamma \sqsubset \beta$ or $\alpha \parallel \gamma$. Again, since $\alpha \parallel \gamma$ implies $\beta \parallel \gamma$, it must hold that $\gamma 1 \sqsubseteq \beta$. Distinguishing the relative position of α to γ there are three possibilities:

1. $\alpha \sqsubset \gamma \sqsubset \beta$: By SD3 the relation U is scopic in t, meaning, from $(\alpha, \beta) \in U$ it follows that $\alpha\, U\, \gamma$ or $\gamma\, U\, \beta$. The latter results in a contradiction to SD4 and the former implies by Lemma 6.2.5 a smaller step contradicting the minimality of γ according to $<_{\text{rev}}$.

2. $\alpha = \gamma$: Equality of α and γ contradicts SD4.

3. $\gamma 1 \sqsubseteq \alpha$: By Lemma 6.2.5 there exists a step, which, as well, contradicts the minimality of γ according to $<_{\text{rev}}$.

Hence, for a step γ minimal according to $<_{\text{rev}}$ it holds that $\gamma 0 \sqsubseteq \beta \vee \alpha \parallel \gamma$. □

Now it is easy to show that for a trek (t, U) the cardinality of U decreases by one traced under a minimal single-step of U.

Lemma 6.3.7. *Let $(s, U) \to_{rev} (t, V)$, then $|V| = |U| - 1$.*

Proof. Let $(\gamma, \gamma 0) \in U$ be the smallest step according to $<_{\text{rev}}$ among all steps in U. Obviously, $\{(\gamma, \gamma 0)\}_{[[\gamma\rangle\rangle} = \emptyset$, since the sp-trace of a position pair is a subset of $\sqsubset$. We show, that for all other pairs $(\alpha, \beta) \in U$ the sp-trace $\{(\alpha, \beta)\}_{[[\gamma\rangle\rangle}$ consists of exactly one pair.

Let $(\alpha, \beta) \in U$ be distinct from $(\gamma, \gamma 0)$. Since γ is minimal according to $<_{\text{rev}}$ it follows by Lemma 6.3.6 that $\gamma 0 \sqsubseteq \beta$ or $\alpha \parallel \gamma$. The latter implies $\beta \parallel \gamma$ and therefore $\{(\alpha, \beta)\}_{[[\gamma\rangle\rangle} = \{(\alpha, \beta)\}$. For the former, note, that for $\beta \in \{\gamma 0, \gamma 00\delta, \gamma 01\delta\}$ with $\delta \in \mathcal{P}os$ it holds that $|(\beta[[\gamma\rangle\rangle)| = 1$. Thus, the same holds for the pair (α, β), i.e., $|\{(\alpha, \beta)\}_{[[\gamma\rangle\rangle}| = 1$.

Hence, for one pair the trace is always empty and all other pairs result in a set consisting of one pair. We conclude by $|U| > |V|$ for $(s, U) \to_{\text{rev}} (t, V)$. The equality $|V| = |U| - 1$ follows from the fact that $\beta_1 \neq \beta_2$ implies $(\beta_1[[\gamma\rangle\rangle) \cap (\beta_2[[\gamma\rangle\rangle) = \emptyset$. □

As a direct consequence of the previous lemma we get weak normalisation, which we state in the following corollary.

Corollary 6.3.8. *Developments of treks are weakly normalizing.*

Proof. Since the norm $\|(t, U)\| := |U|$ is strictly decreasing for $\to_{\text{rev}}$, the strategy is terminating. □

To show strong normalization we introduce the size of a term, which corresponds to the number of function symbols.

Definition 6.3.9. Let t be a term. Define the size of t by

$$|t| = \begin{cases} 0 & \text{if } t \text{ is a variable} \\ 1 + |t_0| + |t_1| & \text{if } t = t_0 \cdot t_1. \end{cases}$$

Since the size of a term increases under a single-step, it poses an increasing function for treks, which is stated in the next lemma.

Lemma 6.3.10. *Developments of treks are increasing.*

Proof. By a simple structural induction on proof terms $\phi : s \geq_{\mathcal{T}_{SD}} t$ it follow that $|s| < |t|$, since a single-step consists of exactly one rule symbol and for $\rho(s_0, s_1, s_2) : s \to_{SD} t$ it holds that $|s| = 2 + |s_0| + |s_1| + |s_2| < 3 + |s_0| + |s_1| + 2|s_2| = |t|$. Then, defining $|(s, U)| := |s|$ the claim follows for developments, since developments are compositions of single-steps. □

Having done all preparatory work, the following theorem states the main result of this section, namely completeness of developments, paving the path to a residual system for SD.

Theorem 6.3.11. *Developments of treks are complete.*

Proof. By Theorem 6.2.12 treks are locally confluent, by Corollary 6.3.8 treks are weakly normalizing, hence, having treks as objects so are developments. Furthermore, by Lemma 6.3.10 developments are increasing. Thus, by Theorem 2.2.15 developments are terminating and with Newman's Lemma completeness follows. □

Remark 6.3.12. With $\to_{\text{rev}}$ we also found an optimal[1] strategy. This is a direct consequence of Lemma 6.3.7, since each pair in U is traced to at least one pair in V for a step $\phi : (s, U) \to_{\text{rev}} (t, V)$ except for the pair $\mathcal{RP}air(\phi) \in U$.

Interestingly, the dual strategy $\to_{\text{ino}}$ that applies the smallest step α according to the in-order tree traversal is maximal[2]. One way to check this provides van Oostrom's ordered local commutation [24]. He defines $\to_{SD}$ ordered locally commutes with $\to_{\text{ino}}$, if $t_1 \leftarrow_{SD} s \to_{\text{ino}} t_2$ implies either t_2 has no $\to_{SD}$-normal form or $t_1 \to_{\text{ino}}^n t \leftarrow_{SD}^m t_2$ with $n \leq m$. It is abbreviated by OLCOM($\to_{SD}, \to_{\text{ino}}$). He further shows that, if OLCOM($\to_{SD}, \to_{\text{ino}}$) then $\to_{\text{ino}}$ is maximal.

[1] A strategy $\rightarrowtail$ is optimal, if for any term s the length of any $\rightarrowtail$-reduction from s to any normal from t is minimal among all possible reductions from s to t.

[2] A strategy $\rightarrowtail$ is maximal, if the minimal number of $\rightarrowtail$-steps needed to reach a normal form is maximal among all reductions to normal form for any term.

To show OLCOM($\to_{SD}, \to_{\text{ino}}$) we distinguish the relative position of α and γ for an arbitrary SD-step $\alpha : s \to_{SD} t_1$ and an SD-step according to in-order $\gamma : s \to_{\text{ino}} t_2$. If $\alpha = \gamma$ the steps are equivalent and $t_1 = t_2$. If $\alpha \parallel \gamma$ the position γ stays the smallest position according to the in-order tree traversal, even after we have done an SD-step at position α, hence on both sides of the digram we can find a common reduct in one step, i.e., $n = 1 = m$. If $\alpha \sqsubseteq \gamma$ it either is the situation of Figure 6.4, i.e., $n = 2 \leq 3 = m$ or γ is further down in the left subtree of α, where in all cases we have $n = m$. If $\gamma \sqsubseteq \alpha$ it holds that α is in the right subtree of γ and it follows that $n = 1 \leq 2 = m$.

Similarly, we could check the claim above and give a second prove of afore-mentioned optimality of $\to_{\text{rev}}$ by showing OLCOM($\to_{\text{rev}}, \to_{SD}$). For further details we refer the reader to the paper of van Oostrom as this is a very brief remark [24].

6.4 A Residual System for Self-Distributivity

In Section 6.3 completeness of developments was shown, which we will be using in this section to define a rewrite system having treks as steps, where sources and targets correspond to a complete development. The fact that non-complete developments can always be extended to complete developments is then, similar to associativity, the key ingredient for proving the cube identity R1. Thus, we first introduce said rewrite system and a corresponding join.

Definition 6.4.1. Define by $\multimap\!\!\!\!\to_{SD}$ the rewrite system consisting of steps defined by treks, such that the source and the target of (s, U) is the source and the target of a complete development of (s, U). We write $(s, U) : s \multimap\!\!\!\!\to_{SD} t$ and define $(s, \emptyset)$ as the empty-step.

Remark 6.4.2. By Theorem 6.3.11 developments are complete, i.e., confluent and terminating, meaning, that for two complete developments ϕ, ψ of (t, U) it holds that $\text{tgt}(\phi) = \text{tgt}(\psi)$, i.e., the target of a trek is well-defined. Moreover, by completeness each trek (t, U) induces a unique trace relation $[[U\rangle\rangle$ relating positions in the source and the target of (t, U).

Definition 6.4.3. The join $\sqcup$ of two co-initial treks $(t, U), (t, V)$ is defined by $(t, U) \sqcup (t, V) := (t, (U \cup V)^+)$.

Next, we will show that the diagonals of the diamonds are part of the rewrite system, i.e., that the join is a trek as well.

Lemma 6.4.4. *Let (t, U) and (t, V) be two co-initial treks, then the join $(t, U) \sqcup (t, V)$ is a trek as well.*

Proof. SD1: Since $U, V \subseteq t$ it follows by Lemma 2.1.9 that $(U \cup V)^+ \subseteq t$. SD2: by definition of transitive closure. SD3: Since t is a tree and U, V are scopic in t, it follows by Theorem 3.2.6 that $(U \cup V)^+$ is scopic as well. SD4: Assume there exists $(\alpha, \alpha 1 \beta) \in (U \cup V)^+ := W$. Since (t, U) and (t, V) are treks there exists $\gamma, \delta \in \mathcal{P}os_\Sigma(t)$, such that $\{(\alpha, \gamma), (\delta, \alpha 1 \beta)\} \subseteq U \cup V$ and a chain $\gamma\ W \ldots W\ \delta$. Since t is a tree it holds that $\alpha \sqsubset \gamma \sqsubset \delta \sqsubset \alpha 1\beta$, meaning, there exists β', such that $\gamma = \alpha 1 \beta'$ contradicting $(t, U), (t, V)$ being treks. ☐

Introducing a binary function on treks and showing that this function is a residuation poses the last step before defining a residual system for SD.

Lemma 6.4.5. *Let $(s, U), (s, V)$ be two co-initial treks. The function $/_{SD}$ defined by $(s, V)/_{SD}(s, U) := (t, (U \cup V)^+[[U\rangle\rangle)$ is a residuation for $\multimap\!\!\!\!\rightarrow_{SD}$, where $s\ [[U\rangle\rangle\ t$.*

Proof. Since $U \subseteq (U \cup V)^+$ there exists a (not necessarily complete) development of $(s, (U \cup V)^+)$ with the steps taken completely developing (s, U), i.e., $\mathrm{tgt}(s, U) = \mathrm{src}(t, (U \cup V)^+[[U\rangle\rangle) = \mathrm{src}((t, U)/_{SD}(t, V))$. Furthermore, note that by (repeatedly applying) Lemma 6.2.8 $(s, (U \cup V)^+[[U\rangle\rangle)$ is a trek again. Hence, by co-finality of complete developments and by commutativity of the join the equality $\mathrm{tgt}((t, U)/_{SD}(t, V)) = \mathrm{tgt}((t, V)/_{SD}(t, U))$ holds. ☐

With the next statement the main goal of this master thesis is presented, namely a residual system for self-distributivity.

Theorem 6.4.6. *$\langle \multimap\!\!\!\!\rightarrow_{SD}, 1, /_{SD} \rangle$ constitutes a residual system for the residuation defined in Lemma 6.4.5.*

Proof. That $/_{SD}$ is a residuation for $\multimap\!\!\!\!\rightarrow_{SD}$ was shown in Lemma 6.4.5. The laws R2–R4 are trivial. To see that the cube identity R1 also holds note, that each trek defines a trace relation. In Lemma 6.4.5 we saw that the corresponding proof term algebra $\mathfrak{A}$ is a model for the diamonds. Hence, for two co-initial treks ψ, χ it holds that $\psi \cdot (\chi/_{SD}\psi) =_{\mathfrak{A}} \chi \cdot (\psi/_{SD}\chi)$, meaning, both sides result in the same trace relation. Hence, a further co-initial trek ϕ after completely developing either path of the diamond results in the same trek, i.e., $(\phi/_{SD}\psi)/_{SD}(\chi/_{SD}\psi) = (\phi/_{SD}\chi)/_{SD}(\psi/_{SD}\chi)$. ☐

Confluence of $\multimap\!\!\!\!\rightarrow_{SD}$ follows from the residuation $/_{SD}$. Confluence of $\mathcal{T}_{SD}$ is easily established completely developing a trek into single-steps. Since the residuation $/_{SD}$ fulfils R1–R4 it yields the least common reduct according to $\multimap\!\!\!\!\rightarrow_{SD}$.

7 Conclusion

This master thesis showed that self-distributivity is orthogonal in the semantic sense of having a residual system (as defined in Terese [23, Section 8.7]). This was done by abstracting from the constructions of residual systems for the S-combinator, associativity and braids.

First, statements about Melliès' scopic relations [17] were generalized to make them applicable to our purposes. Then treks were introduced, extending the definition of a braid multi-step. The derivation of a residual system for self-distributivity was done by developments over treks, analogue to associativity. Here, a crucial role played the concept of tracing as introduced in Terese [23, Section 8.6]. Showing termination of developments over treks was proven by the increasingness-theorem using a normalizing strategy. This bears similarities to the also duplicating term rewrite system of the S-combinator considering the inductive definition of a residual as a normalizing, innermost strategy. That the finally obtained residual system for self-distributivity indeed fulfils the cube law and the unit identities was verified by the fact that the proof term algebra defined by the trace relations over treks acts as a model for the diamond.

Furthermore, we remarked that developing a trek according to the reversed in-order tree traversal formulates an optimal strategy. On the contrary, developing according to the in-order tree traversal results in a maximal strategy.

Future Work

Parallel reductions in λ-calculus as defined by Tait & Martin-Löf and later refined by Takahashi opened the opportunity to inductive proofs [22], since they are defined on the structure of λ-terms. Similarly the theory involving self-distributivity could simplify and benefit from an inductive definition for the target of a trek's complete development. So far, attempts by the author remained unsuccessful. As a starting point could serve Dehornoy's dilatation operator, inductively defining a common reduct of all possible single SD-steps of a term [8, Definition V.3.8].

Bibliography

[1] Emil Artin. Theorie der Zöpfe (German) [Theory of braids]. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 4(1):47–72, 1926. doi:10.1007/BF02950718.

[2] Franz Baader and Tobias Nipkow. *Term rewriting and all that*. Cambridge University Press, 1998. doi:10.1017/CBO9781139172752.

[3] Henk P. Barendregt. *The lambda calculus - its syntax and semantics*, volume 103 of *Studies in logic and the foundations of mathematics*. North Holland, Amsterdam, Nex York, Oxford, 1984. 2nd edition.

[4] Stanley Burris and Hanamantagouda P. Sankappanavar. *A course in universal algebra*, volume 78 of *Graduate texts in mathematics*. Springer, Berlin, 1981.

[5] Scott Carter. A survey of quandle ideas. In Louis H. Kauffman, Sofia Lambropoulou, Slavik Jablan, and Jozef H. Przytycki, editors, *Introductory lectures on Knot Theory*, volume 46 of *Series on Knots and Everything*, pages 22–53. World Scientific, September 2011. doi:10.1142/7784.

[6] Scott Carter, Daniel Jelsovsky, Seiichi Kamada, Laurel Langford, and Masahico Saito. Quandle cohomology and state-sum invariants of knotted curves and surfaces. *Transactions of the American Mathematical Society*, 355(10):3947–3989, 2003. doi:10.1090/S0002-9947-03-03046-0.

[7] Scott Carter, Seiichi Kamada, and Masahico Saito. Geometric interpretations of quandle homology. *Journal of Knot Theory and Its Ramifications*, 10(03):345–386, 2001. doi:10.1142/S0218216501000901.

[8] Patrick Dehornoy. *Braids and Self-Distributivity*, volume 192 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, Boston, Berlin, 2000. doi:10.1007/978-3-0348-8442-6.

[9] Patrick Dehornoy. Some aspects of the sd-world. *Contemporary Mathematics*, 721:69–96, 2019. doi:10.1090/CONM/721.

[10] Jörg Endrullis and Jan W. Klop. Braids via term rewriting. *Theoretical Computer Science*, 777:260 – 295, 2019. doi:10.1016/J.TCS.2018.12.006.

[11] James L. Hein. *Discrete Structures, Logic, and Computability*. Jones and Bartlett Publishers, Inc., Boston, Toronto, London, Singapore, 2010. 3rd edition.

[12] Nao Hirokawa, Julian Nagele, Vincent van Oostrom, and Michio Oyamaguchi. Confluence by critical pair analysis revisited. In Pascal Fontaine, editor, *27th International Conference on Automated Deduction (CADE2019), Natal, Brazil, Proceedings*, volume 11716 of *Lecture Notes in Computer Science*, pages 319–336. Springer, August 2019. `doi:10.1007/978-3-030-29436-6_19`.

[13] Ayumu Inoue and Yuichi Kabaya. Quandle homology and complex volume. *Geometriae Dedicata*, 171(1):265–292, 2013. `doi:10.1007/S10711-013-9898-2`.

[14] Jan W. Klop. *Combinatory reduction systems*. Thesis (doctoral), Rijksuniversiteit Utrecht, June 1980.

[15] Jan W. Klop, Vincent van Oostrom, and Roel C. de Vrijer. *Course Notes on Braids*. University of Utrecht and CWI, July 1998. Draft, 45 pages. Available on the authors' webpage.

[16] Paul-André Melliès. Axiomatic rewriting theory VI: Residual theory revisited. In Sophie Tison, editor, *13th International Conference on Rewriting Techniques and Applications (RTA2002), Copenhagen, Denmark, Proceedings*, volume 2378 of *Lecture Notes in Computer Science*, pages 24–50. Springer, July 2002. `doi:10.1007/3-540-45610-4_4`.

[17] Paul-André Melliès. Braids described as an orthogonal rewriting system. *Festschrift in Honour of Roel de Vrijer*, based on notes from 1995, released 2009.

[18] José Meseguer. Conditional rewriting logic as a unified model of concurrency. *Theoretical Computer Science*, 96(1):73–155, 1992. `doi:10.1016/0304-3975(92)90182-F`.

[19] Enno Ohlebusch. *Advanced topics in term rewriting*. Springer, 2002. `doi:10.1007/978-1-4757-3661-8`.

[20] Pierre Rosenstiehl and George Th. Guilbaud. Analyse algébrique d'un scrutin (French) [Algebraic analysis of a ballot]. In *Ordres totaux finis*, pages 72–100. Paris, Gauthier-Villars et Mouton, 1971.

[21] Moses Schönfinkel. Über die Bausteine der mathematischen Logik (German) [On building blocks of mathematical logic]. *Mathematische Annalen*, 92:305–316, 1924. `doi:10.1007/BF01448013`.

[22] Masako Takahashi. Parallel reductions in λ-calculus. *Information and Computation*, 118(1):120–127, 1995. `doi:10.1006/inco.1995.1057`.

[23] Terese. *Term rewriting systems*, volume 55 of *Cambridge tracts in theoretical computer science*. Cambridge University Press, 2003.

[24] Vincent van Oostrom. Random descent. In Franz Baader, editor, *18th International Conference on Term Rewriting and Applications (RTA2007), Paris, France, Proceedings*, volume 4533 of *Lecture Notes in Computer Science*, pages 314–328. Springer, June 2007. doi:10.1007/978-3-540-73449-9_24.

[25] Vincent van Oostrom. Multi-redexes and multi-treks induce residual systems least upper bounds and left-cancellation up to homotopy. In Samuel Mimram and Camilo Rocha, editors, *10th International Workshop on Confluence (IWC2021), Buenos Aires, Argentina (online), Proceedings*, pages 1–7, July 2021.

[26] Vincent van Oostrom. Personal communication, 2021.

[27] Vincent van Oostrom. Z; syntax-free developments. In Naoki Kobayashi, editor, *6th International Conference on Formal Structures for Computation and Deduction (FSCD2021), Buenos Aires, Argentina (online), Proceedings*, volume 195 of *LIPIcs*, pages 24:1–24:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, July 2021. doi:10.4230/LIPIcs.FSCD.2021.24.

[28] Vincent van Oostrom and Roel C. de Vrijer. Four equivalent equivalences of reductions. *Electronic Notes in Theoretical Computer Science*, 70(6):21–61, 2002. doi:10.1016/S1571-0661(04)80599-1.

[29] Johannes Waldmann. The combinator S. *Information and Computation*, 159(1-2):2–21, 2000. doi:10.1006/INCO.2000.2874.