1

Abstract Rewriting and 1-Dimensional Polygraphs

We begin by discussing 1-polygraphs, which are simply directed graphs, thought of here as abstract rewriting systems: they consist of vertices, which represent the objects of interest, and arrows, which indicate that we can rewrite one object into another. After formally introducing those in Section 1.1, we will see in Section 1.2 that they provide a notion of *presentation* for sets, by generators and relations. Of course, presentations of sets are of little interest in themselves, but they are merely used here as a gentle introduction to some of the main concepts discussed in this work: in particular, we introduce the notion of Tietze transformations which generate the equivalence between two presentations of the same set. In this context, an important question consists in deciding when two objects are equivalent, i.e., represent the same element of the presented set. In order to address it, we develop the theory of abstract rewriting systems in Section 1.3. Most notably, we show that when the rewriting system satisfies the two properties of *termination* and *confluence*, equivalence classes of objects admit a unique canonical representative, the *normal form*, and equivalence of objects can thus be decided by comparing the associated normal forms. Finally, in Section 1.4, we detail the more advanced method of decreasing diagrams, which can be used to show confluence in the absence of termination.

1.1 The Category of 1-Polygraphs

A 0-*polygraph* is simply another name for a set. Since there is not much to do with those, we move on to 1-polygraphs.

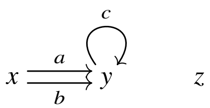
1.1.1 Definition. A 1-*polygraph* P consists of a 0-polygraph P_0, whose elements are called 0-*generators*, together with a set P_1 of 1-*generators* and two functions $s_0^P, t_0^P : P_1 \to P_0$ respectively associating to each 1-generator its

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

source and *target* 0-cell. We often write $\langle P_0 \mid P_1 \rangle$ for such a polygraph and $a\colon x \to y$ for a 1-generator a in P_1 such that $s_0^P(a) = x$ and $t_0^P(a) = y$. A 1-polygraph P is *finite* when both P_0 and P_1 are.

The notion of 1-polygraph is simply another name for the notion of *graph*, by which we always mean a directed multigraph, which we sometimes also call a 1-*graph*. Indeed, a polygraph P as above is a graph with P_0 as set of vertices P_1 as set of edges, an edge $a \in P_1$ having $s_0^P(a)$ as source and $t_0^P(a)$ as target. Thus, any terminology pertaining to oriented graphs, such as the notion of *path*, immediately applies to 1-polygraphs.

1.1.2 Example. The directed graph



(1.1)

can be encoded as the 1-polygraph P with $P_0 = \{x, y, z\}$, $P_1 = \{a, b, c\}$ and

$$s_0(a) = s_0(b) = x, \qquad t_0(a) = t_0(b) = y, \qquad s_0(c) = t_0(c) = y,$$

which can be more concisely denoted as

$$P = \langle\, x, y, z \mid a\colon x \to y, b\colon x \to y, c\colon y \to y \,\rangle\,.$$

1.1.3 The category of 1-polygraphs. A *morphism* $f\colon P \to Q$ between 1-polygraphs P and Q consists of a pair of functions $f_0\colon P_0 \to Q_0$ and $f_1\colon P_1 \to Q_1$ respectively sending the 0- and 1-cells of P to those of Q and preserving sources and targets:

$$s_0^Q \circ f_1 = f_0 \circ s_0^P, \qquad\qquad t_0^Q \circ f_1 = f_0 \circ t_0^P.$$

We write $\mathbf{Pol}_1$ for the category of 1-polygraphs and their morphisms. Again, this is simply another name for the usual category of directed graphs and their morphisms.

1.2 Presenting Sets

A 1-polygraph P can be seen as a *presentation* of a set X, in the following sense. Each element x of P_0 denotes an element $\overline{x}$ of X, in such a way that each element of X has at least one "name" in P_0, and each element $a\colon x \to y$ in P_1 represents the renaming of $\overline{x}$ by $\overline{y}$. The elements of P_0 and P_1 are often respectively called *generators* and *relations*.

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

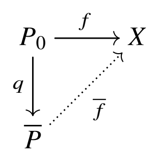
1.2.1 *P*-congruence. The *P-congruence* $\approx^P$ associated with a 1-polygraph P is the smallest equivalence relation on P_0 such that $x \approx^P y$ for every 1-generator $a\colon x \to y$ in P_1.

1.2.2 The presented set. The *set* $\overline{P}$ *presented* by a 1-polygraph P is the set $P_0/{\approx^P}$ obtained by quotienting P_0 by the P-congruence $\approx^P$, what we usually simply write P_0/P_1. More generally, a set X is *presented* by a 1-polygraph P when X is isomorphic to $\overline{P}$, and in this case P is called a *presentation* of X. Geometrically speaking, X amounts to the set of connected components of the graph P.

1.2.3 Example. In Example 1.1.2, the relation $\approx^P$ identifies x and y, and the presented set is the set with two elements, corresponding to the equivalence classes $\{x, y\}$ and $\{z\}$.

More abstractly, the set presented by a 1-polygraph P can be characterized by the following universal property:

1.2.4 Lemma. *For any set X and function $f\colon P_0 \to X$ such that $f(x) = f(y)$ for every* 1*-generator $a\colon x \to y$ in P_1, there exists a unique function $\overline{f}\colon \overline{P} \to X$ such that $\overline{f} \circ q = f$*



,

where $q\colon P_0 \to \overline{P}$ is the function sending an element to its equivalence class.

1.2.5 Tietze transformations. At this point, a natural question to ask is: when do two polygraphs present the same set? For instance, the set with two elements can also be presented by the polygraph

$$x \xrightarrow{d} x' \xrightarrow{e} y \qquad\qquad z \tag{1.2}$$

which looks quite different from (1.1), and it is not obvious how the two are related. This question was first studied by Tietze for presentations of groups [345], as we shall see in Chapter 5, but similar results already hold for plain sets as we now explain.

We call *elementary Tietze transformations* the following operations transforming a 1-polygraph P into a 1-polygraph Q:

(T1) *adding a definable generator*: given $x \in P_0$, $y \notin P_0$, and $a \notin P_1$, we define

$$Q = \langle\, P_0, y \mid P_1, a\colon x \to y \,\rangle,$$

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

(T2) *adding a derivable relation*: given $x, y \in P_0$ and $a \notin P_1$ such that $x \approx^P y$, we define

$$Q = \langle\, P_0 \mid P_1, a\colon x \to y \,\rangle.$$

A *Tietze transformation* from P to Q is a zigzag of elementary Tietze transformations, i.e., a finite sequence of polygraphs $(P_i)_{0\leqslant i\leqslant n}$ with $P_0 = P$ and $P_n = Q$, together with, for each index $0 \leqslant i < n$, an elementary Tietze transformation either from P_i to P_{i+1} or from P_{i+1} to P_i. The *Tietze equivalence* is the smallest equivalence relation on 1-polygraphs, identifying any two polygraphs related by an elementary Tietze transformation and closed by isomorphism; otherwise said, two polygraphs are Tietze equivalent when there exists a Tietze transformation between them, up to isomorphism.

1.2.6 Lemma. *Two Tietze equivalent* 1*-polygraphs present isomorphic sets.*

Proof. By induction on the length of Tietze transformations, it is enough to show that two polygraphs P and Q related by an elementary Tietze transformation present the same set. Using the same notations as above, in the case of the transformation (T1), we have

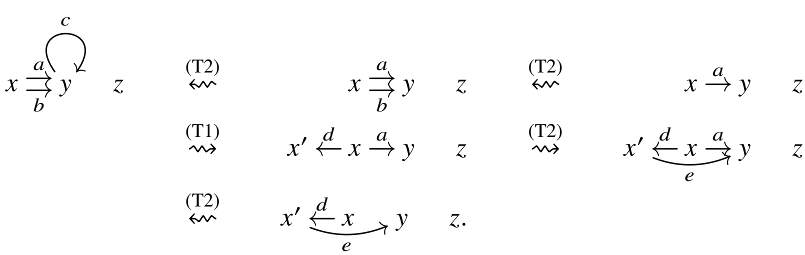
$$\overline{Q} = (P_0 \sqcup \{y\})/{\approx^Q} = ((P_0 \sqcup \{y\})/(x \approx y))/{\approx^P} = P_0/{\approx^P} = \overline{P},$$

where $x \approx y$ denotes the smallest equivalence relation identifying x and y. In the case of the transformation (T2), the relations generated by P_1 and Q_1 are the same and we have

$$\overline{Q} = Q_0/{\approx^Q} = P_0/{\approx^P} = \overline{P}.$$ □

We will see in Theorem 1.2.12 that the converse also holds: these operations exactly axiomatize when two finite 1-polygraphs are presenting the same set.

1.2.7 Example. Using the above lemma, one can deduce that the two polygraphs (1.1) and (1.2) present the same set, by building a series of Tietze transformations relating them:



In the first step, $y \approx y$ can be shown without resorting to the relation $c\colon y \to y$ (this is because, by definition, $\approx$ is an equivalence relation), and therefore the

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

relation h can be removed using the Tietze transformation (T2) backward. Other steps can be justified similarly. Of course, in this case, it is very easy to compute the sets presented by the two polygraphs (1.1) and (1.2) and to see that they are isomorphic (both have two elements), but it will no longer be the case when generalizing to higher dimensions.

1.2.8 Backward Tietze transformations. A Tietze transformation is a zigzag of elementary Tietze transformations. It can alternatively be seen as a sequence of elementary Tietze transformations or the following transformations, that we call *backward elementary Tietze transformations*, corresponding to using an elementary Tietze transformation in the "backward direction":

$\overline{\text{(T1)}}$ *removing a definable generator*: given a polygraph P of the form

$$P = \langle\, P'_0, x \,|\, P'_1, a\colon x \to y \,\rangle,$$

where x does not occur in any relation of P'_1, we define

$$Q = \langle\, P'_0 \,|\, P'_1 \,\rangle,$$

$\overline{\text{(T2)}}$ *removing a derivable relation*: given a polygraph P of the form

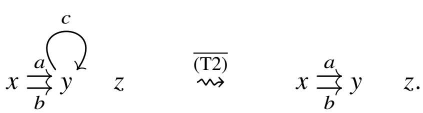
$$P = \langle\, P_0 \,|\, P'_1, a\colon x \to y \,\rangle,$$

we define

$$Q = \langle\, P_0 \,|\, P'_1 \,\rangle$$

whenever $x \approx^{Q} y$.

1.2.9 Remark. Given an elementary Tietze transformation from P to Q, there is an obvious inclusion of P into Q that induces a morphism of 1-polygraphs $P \to Q$. However, for a backward elementary Tietze transformation from P to Q there is no canonical morphism $P \to Q$. For instance, consider the transformation



The only reasonable choice would be to send the 1-generator $c\colon y \to y$ to an identity on y, which is not possible with a morphism of 1-polygraph (those send 1-generators to 1-generators). This is one of the reasons why we take the elementary Tietze transformations (as opposed to the backward ones) as more primitive.

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

1.2.10 Minimal presentations. It can be noted that Tietze transformations consisting only of elementary transformations (T1) and (T2) make the presentations larger (in terms of number of generators and relations), whereas those consisting only of $\overline{\text{(T1)}}$ and $\overline{\text{(T2)}}$ make them smaller. We thus sometimes respectively call *Tietze expansions* and *Tietze reductions* these two families of Tietze transformations and say that a polygraph P *Tietze expands* (resp. *Tietze reduces*) to a polygraph Q if Q can be obtained from P by applying a series of Tietze expansions (resp. Tietze reductions). One may wonder if, by applying only the second kind of transformations, we eventually always reach a *minimal* presentation with respect to both generators and relations, and whether two such minimal presentations are necessarily isomorphic. We will see that it is indeed the case for finite polygraphs. First, note that a 1-polygraph P without relations (i.e., $P_1 = \emptyset$) is always minimal.

1.2.11 Lemma. *Any finite* 1*-polygraph P Tietze reduces to a polygraph isomorphic to $\langle\, \overline{P} \mid \,\rangle$.*

Proof. By induction on the cardinal of P_1, we show that we can remove a 1-generator using Tietze transformations, unless P_1 is empty. Suppose that P contains a non-directed cycle, i.e., a non-empty non-directed path from a 0-generator x to itself. We can assume that this path does not use the same edge twice; otherwise, we can choose a smaller cycle. Given a 1-generator $a\colon x \to y$ occurring in this cycle, there exists a non-directed path from x to y that is not using a. Therefore, we can apply a Tietze transformation $\overline{\text{(T2)}}$ to remove a. Otherwise, there is no cycle, and consider a maximal non-directed path in P. Since P is finite and acyclic, this path will end by a 1-generator $a\colon x \to y$ such that either x or y is incident to no other edge. Therefore, we can use a Tietze transformation $\overline{\text{(T1)}}$ to remove x or y, along with a. □

In the case of *finite* 1-polygraphs, the above lemma implies the converse of Lemma 1.2.6:

1.2.12 Theorem. *Two finite* 1*-polygraphs present isomorphic sets if and only if they are Tietze equivalent.*

Proof. Suppose given two polygraphs P and Q such that $\overline{P} \simeq \overline{Q}$. By the previous lemma, P is Tietze equivalent to $\langle\, \overline{P} \mid \,\rangle$, and similarly Q is Tietze equivalent to $\langle\, \overline{P} \mid \,\rangle$. Finally, the presentations $\langle\, \overline{P} \mid \,\rangle$ and $\langle\, \overline{Q} \mid \,\rangle$ are easily seen to be Tietze equivalent because $\overline{P}$ and $\overline{Q}$ are isomorphic. □

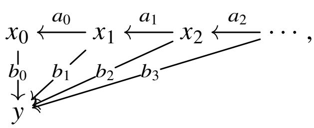
1.2.13 Remark. Note that, given the above definition of Tietze transformations, the previous theorem does not generalize to infinite presentations. For instance, the 1-polygraphs $\langle\, x \mid \,\rangle$ and $\langle\, x_i \mid a_i\colon x_i \to x_0 \,\rangle_{i\in\mathbb{N}}$ both present the set with

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

one element but are not Tietze equivalent since we can only add or remove a finite number of relations using Tietze equivalences (the notation on the right means that i ranges over $\mathbb{N}$ both in generators x_i and relations a_i). In order to overcome this counter-example, one might be naively tempted to allow infinite sequences of Tietze transformations between 1-polygraphs, but this does not preserve presented sets. For instance, consider the 1-polygraph

$$\langle\, x_i, y \mid a_i : x_{i+1} \to x_i, b_i : x_i \to y \,\rangle_{i \in \mathbb{N}},$$

i.e., the graph



presenting the set with one element. Using Tietze transformations, any finite number of relations b_i can be removed from the polygraph, since they are derivable. However, if we remove all of them the resulting polygraph presents the set with two elements.

In order to account for infinite presentations, the notion of Tietze equivalence has to be generalized as follows. Firstly, we say that a 1-polygraph P Tietze expands to Q if there is a transfinite sequence of elementary Tietze expansions from P to Q; secondly, we define Tietze equivalence as the smallest equivalence relation containing Tietze expansions. Two (not necessarily finite) 1-polygraphs are Tietze equivalent in this sense if and only if they present isomorphic sets. We do not dwell further on infinite polygraphs, because we are mostly interested in finite polygraphs in this book; details can be found in [178].

We will see that Lemma 1.2.11 does not generalize in dimensions higher than 1, where arbitrary finite sequences of Tietze transformations, interleaving Tietze reductions and expansions, might be required in order to show that two polygraphs present the same object. However, an analogous of Theorem 1.2.12 will still hold, but its proof has to be carried over differently, as explained in Chapter 5.

1.3 Abstract Rewriting Systems

The orientations of the relations do not really matter in a 1-polygraph, with respect to the presented set: if we reverse an edge, the presented set is the same. This is easily shown using the following series of Tietze transformations:

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

$$\langle\, P_0 \mid P'_1, x \to y \,\rangle \overset{(T2)}{\rightsquigarrow} \langle\, P_0 \mid P'_1, x \to y, y \to x \,\rangle \overset{\overline{(T2)}}{\rightsquigarrow} \langle\, P_0 \mid P'_1, y \to x \,\rangle,$$

which are based on the fact that $\approx$ is an equivalence relation and thus symmetric.

However, the orientations can still be useful to *decide equality* between generators, i.e., answer the following question:

> Given two generators, do they represent the same element of the presented set? Or, equivalently, are they related by $\approx$?

We will see that in good cases, one can come up with canonical representatives of equivalence classes under $\approx$, in such a way that the representative of an arbitrary generator can easily be computed. In those situations, the equivalence of two generators can be tested by checking whether their representatives are equal or not. In order to come up with representatives, we use the orientation of the 1-generators. Given two 0-generators x and y such that there is a 1-generator $a\colon x \to y$, we have $x \approx y$, and the orientation of the 1-generator will be interpreted as indicating that y is a "more canonical" representative than x in the equivalence class under $\approx$. With respect to this, the "most canonical" elements, which are called normal forms, are good candidates for being representatives of equivalence classes with good properties: under reasonable assumptions, it can be shown that every class admits exactly one such representative. This point of view is the starting point of *rewriting theory* [20, 342].

1.3.1 Terminology and notations. We have seen that a 1-polygraph P is simply another name for a graph. Since people in rewriting theory like to think about it from a different point of view, they give it yet another name and call it an *abstract rewriting system*. In this context, the elements of P_0 are called *objects* and those of P_1 are called *rewriting rules* (or *rewriting steps*). A *rewriting path* is simply a path, i.e., a sequence

$$x_0 \xrightarrow{a_1} x_1 \xrightarrow{a_2} x_2 \xrightarrow{a_3} \dots \xrightarrow{a_n} x_n$$

of composable rewriting steps. The 0-cells x_0 and x_n are respectively called the *source* and *target* of the path, and we write $f\colon x \overset{*}{\to} y$ for a path f from x to y. One also writes $x \to y$ (resp. $x \overset{*}{\to} y$) when there exists a rewriting step (resp. a rewriting path) from x to y, and the notation $x \overset{*}{\leftrightarrow} y$ is often used instead of $x \approx y$.

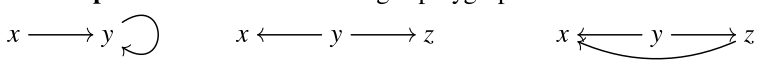
1.3.2 Normal forms. A 0-cell $x \in P_0$ is a *normal form* when there is no rule $a\colon x \to y$ in P_1 with x as source.

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

We can distinguish the following situations concerning normal forms in equivalence classes under $\approx$ of 0-cells in a polygraph P: we say that P has

- the *existing normal form property* when every equivalence class contains at least one normal form; i.e., for every $x \in P_0$ there exists a normal form $y \in P_0$ such that $x \overset{*}{\leftrightarrow} y$;
- the *unique normal form property* when every equivalence class contains at most one normal form; i.e., for every normal form $x, y \in P_0$, $x \overset{*}{\leftrightarrow} y$ implies $x = y$; and
- the *canonical form property* when every equivalence class contains exactly one normal form, called the *canonical representative* of the class; i.e., it satisfies both the existing and the unique normal form property.

1.3.3 Example. Consider the following 1-polygraphs:



(1) (2) (3)

(1) and (3) have the unique normal form property, (2) and (3) have the existing normal form property, and (3) has the canonical form property.

We are interested here in providing practical conditions on P that ensure that the canonical form property holds, as well as that we are able to efficiently compute the canonical form associated to the class of a 0-cell. We will see that termination of a 1-polygraph implies the existing normal form, that confluence implies the unique normal form property, and moreover that confluence can be checked locally for terminating 1-polygraphs.

1.3.4 Normalizability. A polygraph is *normalizing* when every 0-cell x rewrites to a normal form. We sometimes write $\widehat{x}$ for an arbitrary choice of such a normal form. From the definition, we deduce the following result.

1.3.5 Lemma. *A normalizing* 1*-polygraph has the existing normal form property.*

The converse does not hold, as illustrated in Example 1.3.20.

1.3.6 Termination. In practice, in order to show that a 1-polygraph is normalizing, one often uses the following property. A 1-polygraph P is *terminating* (or *well-founded* or *noetherian* or *strongly normalizing*) when there is no infinite sequence of rewriting steps

$$x_0 \xrightarrow{a_1} x_1 \xrightarrow{a_2} x_2 \xrightarrow{a_3} \cdots .$$

For instance, in Example 1.3.3, (2) and (3) are terminating but not (1).

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

Starting from a 0-cell x in a terminating 1-polygraph, we can define a sequence of 0-cells by induction by $x_0 = x$, and x_{i+1} is the target of an arbitrary rewriting rule $x_i \to x_{i+1}$ with x_i as source; we stop if there is no such rewriting rule. Termination ensures that this process will end after a finite number of steps, and the last 0-cell x_n is necessarily a normal form. We have just shown the following.

1.3.7 Lemma. *A terminating* 1*-polygraph is normalizing.*

The converse does not hold, as illustrated in Example 1.3.20.

In practice, the termination of a 1-polygraph P can be shown using the following lemma. We recall that a poset $(N, \leqslant)$ is *well-founded* when every decreasing sequence $n_1 \geqslant n_2 \geqslant \ldots$ is eventually stationary: there exists $k \in \mathbb{N}$ such that for every $i, j \in \mathbb{N}$ with $i \geqslant j \geqslant k$ one has $n_i = n_j$. Equivalently, the poset is well-founded when there exists no infinite strictly decreasing sequence $n_1 > n_2 > \ldots$ of elements of N. The typical example of such an order is $(\mathbb{N}, \leqslant)$, or any ordinal.

1.3.8 Lemma. *Given a rewriting system P the following statements are equivalent.*

1. *The rewriting system P is terminating.*
2. *There exists a well-founded order on P_0 such that $x > y$ for every* 1*-generator $a : x \to y$ in P_1.*
3. *There exists a function $f : P_0 \to N$, where N is a well-founded poset, such that $f(x) > f(y)$ for every* 1*-generator $a : x \to y$ in P_1.*

Proof. Suppose that P is terminating. Then the preorder relation on P_0 defined by $x \geqslant y$ whenever $x \overset{*}{\to} y$ is a well-founded partial order that shows that 1 implies 2, and taking $f : P_0 \to P_0$ to be the identity shows that 2 implies 3. Finally, 3 implies 1, for if there was an infinite reduction sequence in P, the image of the objects under f would be an infinite strictly decreasing sequence of elements of N. □

1.3.9 Well-founded induction. Suppose given a predicate $\mathcal{P}$ on the 0-cells of a terminating polygraph P. In order to show that $\mathcal{P}$ holds all the elements of P_0, it is often useful to use the following *well-founded induction principle*: if

$$\forall x \in P_0, \qquad \big((\forall y \in P_0,\ x \to y \text{ implies } \mathcal{P}(y)) \quad \text{implies} \quad \mathcal{P}(x)\big) \tag{1.3}$$

then $\forall x \in P_0,\ \mathcal{P}(x)$ holds.

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

1.3.10 Proposition. *If P is a terminating 1-polygraph then the well-founded induction principle holds.*

Proof. By contradiction, suppose that the well-founded induction principle does not hold: there is a predicate $\mathcal{P}$, such that the hypothesis (1.3) holds but not the conclusion, i.e., $\mathcal{P}(x_0)$ does not hold for some $x_0 \in P_0$. By repeated use of (1.3), we can construct a family $(x_i)_{i\in\mathbb{N}}$ of elements of P_0 such that $\mathcal{P}(x_i)$ does not hold for any $i \in \mathbb{N}$, and $x_0 \to x_1 \to \cdots$. This contradicts the fact that P is terminating. □

1.3.11 Quasi-termination. Following [111], we introduce the following variant of the termination condition. We say that a 1-polygraph P is *quasi-terminating* if every sequence $(x_i)_{i\in\mathbb{N}}$ of 0-cells, with $x_i \to x_{i+1}$ for every index $i \in \mathbb{N}$, contains an infinite number of occurrences of the same 0-cell: there exists a 0-cell x such that for every $i \in \mathbb{N}$, there exists $j > i$ such that $x_j = x$.

Let P be a 1-polygraph. A 0-cell x is called a *quasinormal form* if for any rewriting step $x \to y$, there exists a rewriting path from y to x. If P is quasi-terminating, any 0-cell x rewrites to a quasi-normal form. Note that this quasi-normal form is neither irreducible nor unique in general. We say that P is *quasi-convergent* if it is confluent and it quasi-terminates.

1.3.12 Example. The following 1-polygraph

$$x \longrightarrow y \rightleftarrows z$$

is quasi-terminating and quasi-convergent. Both y and z are quasi-normal forms.

The above termination and normalizability conditions ensure the existing normal form property. We now investigate conditions implying the unique normal form property.

1.3.13 Joinability. Two 0-cells $x, y \in P_0$ of a polygraph P are *joinable* when there exists 0-cell z such that there are rewriting paths $f : x \overset{*}{\to} z$ and $g : y \overset{*}{\to} z$:

$$x \overset{*}{\dashrightarrow} z \overset{*}{\dashleftarrow} y.$$

1.3.14 The Church–Rosser property. A 1-polygraph P has the *Church–Rosser property* when any two 0-cells $x, y \in P_0$ which are equivalent are joinable:

$$x \overset{*}{\longleftrightarrow} y, \qquad x \overset{*}{\dashrightarrow} z \overset{*}{\dashleftarrow} y.$$

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

1.3.15 Proposition. *A* 1*-polygraph with the Church–Rosser property has the unique normal form property.*

Proof. Suppose given two normal forms x and y such that $x \approx y$. By the Church–Rosser property, there exists a 0-cell z and rewriting paths $x \overset{*}{\to} z$ and $y \overset{*}{\to} z$. Since x and y are normal forms, these two paths are necessarily empty, and thus $x = y$. □

The converse property is not true, as illustrated by the 1-polygraph

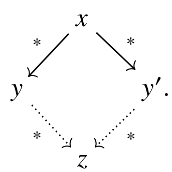
$$x \longleftarrow y \longrightarrow z \circlearrowleft$$

where x and z are equivalent but cannot be rewritten to a common 0-cell, even though there is a unique normal form x.

In the following, we present more "local" properties which imply the Church–Rosser property, and thus the unique normal form property.

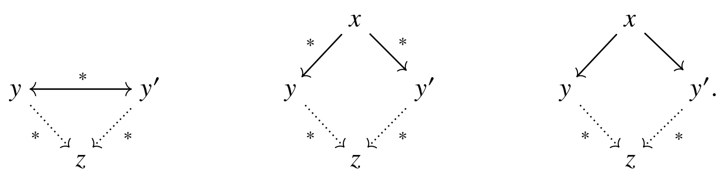
1.3.16 Branchings. In a 1-polygraph P, a pair (a, a') of coinitial 1-generators $a\colon x \to y$ and $a'\colon x \to y'$ in P is called a *local branching*; a pair (f, f') of coinitial rewriting paths $f\colon x \overset{*}{\to} y$ and $f'\colon x \overset{*}{\to} y'$ is called a *branching*. The 0-cell x is called the *source* of the branching.

1.3.17 Confluence. A branching (f, f') as above is *confluent* when y and y' are joinable:



In this situation, we say that the branching is *confluent*. A 1-polygraph is *confluent* (resp. *locally confluent*) when every branching (resp. local branching) is confluent. Note that a confluent 1-polygraph is necessarily locally confluent.

The above confluence conditions can be summarized graphically as follows:

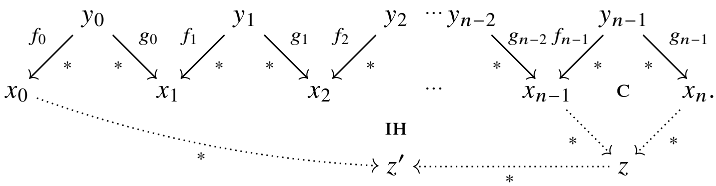


Church–Rosser | confluence | local confluence

1.3.18 Proposition. *A* 1*-polygraph has the Church–Rosser property if and only if it is confluent.*

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

Proof. The left-to-right direction is immediate. For the right-to-left direction, suppose that x and y are two equivalent 0-cells: this means that there exists rewriting paths $f_i : y_i \xrightarrow{*} x_i$ and $g_i : y_i \xrightarrow{*} x_{i+1}$ in P, with $0 \leqslant i < n$, where $x_0 = x$ and $x_n = y$, forming a diagram as below (ignoring the dotted arrows, z and z'):



By induction on $n \in \mathbb{N}$, we show that x_0 and x_n can be joined. The result is immediate when $n = 0$, and otherwise the diagram can be completed as above using the confluence hypothesis for C and the induction hypothesis for IH. ◻

As a direct corollary, we deduce:

1.3.19 Lemma. *A confluent* 1*-polygraph has the unique normal form property.*

Confluence is difficult to show in practice, whereas local confluence is much more tractable. Clearly confluence of a rewriting system implies its local confluence, and one could hope that both properties are equivalent. This is however not the case: local confluence does not imply confluence in general illustrated by the following example attributed by Hindley to Kleene, see [188, Figure 6b] and [342, Section 1.2].

1.3.20 Example. Consider the following 1-polygraph:

$$x' \longleftarrow x \rightleftarrows y \longrightarrow y'.$$

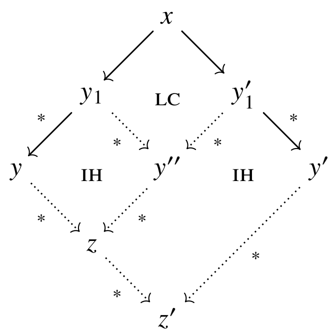
It is locally confluent (it is easy to check all the possible cases), but not confluent: we have $x \xrightarrow{*} x'$ and $x \xrightarrow{*} y'$, but there is no 0-cell to which both x' and y' rewrite.

In the previous example, it can be noted that the rewriting system is not terminating since there is a directed cycle between the vertices x and y. It was shown in a famous lemma by Newman [290], also known as the *diamond lemma*, that local confluence and confluence are equivalent when restricting to terminating rewriting systems, thus providing us with simple ways of checking for their confluence.

1.3.21 Lemma. *A terminating* 1*-polygraph is confluent if and only if it is locally confluent.*

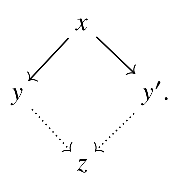
https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

Proof. We show the right-to-left direction, the other one being immediate. We say that a 1-polygraph is *confluent* (resp. *locally confluent*) *at a* 0*-cell* x when every branching (resp. local branching) with x as source is joinable. By well-founded induction, whose use is justified by Proposition 1.3.10 based on the hypothesis that the 1-polygraph is terminating, we show that the local confluence property at a vertex x implies the confluence property at x. The base cases are immediate. Otherwise, we have a diagram of the form



which can be closed using the local confluence hypothesis for LC and the induction hypothesis for IH (which provides confluence at y_1 and y'_1, respectively). □

1.3.22 Remark. Showing termination and local confluence is the most usual way of proving that an abstract rewriting system is confluent, but it is not the only one. We refer to standard rewriting textbooks for other properties which imply confluence [20, 342]. For instance, an abstract rewriting system has the *diamond property* when for every pair of coinitial rewriting steps $a : x \to y$ and $b : x \to y'$ there exists a pair of cofinal rewriting steps (i.e., rewriting paths of length one) $a' : y \to x$ and $b' : y' \to x$. Graphically,



In this case, the abstract rewriting system is always confluent (this can be shown using a variant of the proof of Lemma 1.3.21) even if it is not terminating.

1.3.23 Convergence. A 1-polygraph is *convergent* when it is both terminating and confluent.

1.3.24 Proposition. *A convergent* 1*-polygraph has the canonical form property.*

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

Proof. Suppose given a convergent 1-polygraph. Since it is terminating, it is normalizing by Lemma 1.3.7 and thus has the existing normal form property by Lemma 1.3.5. Since it is confluent, Lemma 1.3.19 ensures that it also has the unique normal form property. □

1.3.25 Remark. A polygraph can have the canonical form property without being convergent:

$$x \rightleftarrows y \longrightarrow z.$$

Here, all the 0-cells are equivalent and z is the only normal form, which shows the canonical form property. The polygraph is not terminating (there is a cycle between x and y) and thus not convergent.

1.3.26 Deciding equality. Give a finite 1-polygraph P, the *equality decision problem*, or the *word problem*, for P consists in answering the following question:

$$\text{Given two 0-cells } x, y \in P_0, \text{ do we have } x \approx y?$$

Since we only consider only finite 1-polygraphs, this problem is *decidable*, meaning that there is a program which takes P, x and y as input and outputs whether $x \approx y$ holds or not. Namely, we can implement a program which will construct all acyclic paths starting from x, which are in finite number, and check whether one of those paths ends at y. We will see that if we assume additional properties on P, this can be performed much more efficiently.

When the 1-polygraph P has the canonical form property, the equivalence class of x (resp. y) contains a unique normal form denoted $\widehat{x}$ (resp. $\widehat{y}$), and we have $x \approx y$ if and only if we have $\widehat{x} = \widehat{y}$. In this case, the equality decision problem can be decided by comparing normal forms. In particular, in the case where the 1-polygraph is convergent, we have seen in Proposition 1.3.24 that it has the canonical form property, and moreover the normal form $\widehat{x}$ associated to a 0-cell x can be computed easily. A maximal path starting from x

$$x = x_0 \xrightarrow{a_0} x_1 \xrightarrow{a_1} x_2 \xrightarrow{a_2} \cdots \xrightarrow{a_{n-1}} x_n$$

exists because P is terminating, and the fact that it is maximal means that its target is a normal form, i.e., $x_n = \widehat{x}$. In order to decide whether x and y are equivalent, we can thus use the *normal form algorithm* which consists in

1. rewriting x as much as possible in order to obtain a normal form $\widehat{x}$, and similarly compute a normal form $\widehat{y}$ for y; and
2. checking whether $\widehat{x} = \widehat{y}$ holds or not.

Formally, this is justified as follows:

1.3.27 Proposition. *In a convergent* 1*-polygraph, two* 0*-cells* x *and* y *are equivalent if and only if they have the same normal form:* $x \approx y$ *if and only if* $\widehat{x} = \widehat{y}$.

Proof. Since the polygraph is terminating, it is normalizing by Lemma 1.3.7: x rewrites to a normal form $\widehat{x}$, and similarly y rewrites to a normal form $\widehat{y}$. If $\widehat{x} = \widehat{y}$, then clearly x and y are equivalent:

$$x \xrightarrow{*} \widehat{x} = \widehat{y} \xleftarrow{*} y.$$

Conversely, suppose that x and y are equivalent, and thus that $\widehat{x}$ and $\widehat{y}$ are also equivalent:

$$\widehat{x} \xleftarrow{*} x \xleftrightarrow{*} y \xrightarrow{*} \widehat{y}.$$

The confluence of the polygraph implies that it has the Church–Rosser property by Proposition 1.3.18, and thus the unique normal form property by Proposition 1.3.15. Since $\widehat{x}$ and $\widehat{y}$ are equivalent normal forms, we deduce that they are equal. □

1.3.28 Deciding confluence. As a direct corollary of the above proposition, we also have a practical method for checking whether a terminating 1-polygraph is confluent (and thus convergent):

1.3.29 Proposition. *A terminating* 1*-polygraph is confluent if and only if for every local branching* $x \to y$ *and* $x \to z$*, we have* $\hat{y} = \hat{z}$.

1.4 Decreasing Diagrams

The main method we have seen so far in order to show the confluence of a 1-polygraph is provided by Newman's lemma (Lemma 1.3.21), which requires supposing termination of the polygraph. As a more advanced topic, we explain here the method of *decreasing diagrams*, introduced by van Oostrom [350], see also [342, Section 14.2], which can be used in order to show the confluence of a 1-polygraph which is non-terminating. Stronger versions of this method have been introduced more recently [126, 351].

1.4.1 Multisets. Given a set A, a *multiset* on A is a function $\mu\colon A \to \mathbb{N}$ which is null almost everywhere, i.e., the set $\{a \in A \mid \mu(a) \neq 0\}$ is finite. The set A is called the *domain* of the multiset. Given an element $a \in A$, the natural number $\mu(a)$ is called its *multiplicity* in the multiset: μ should be thought of as a collection of elements of A where each element a occurs $\mu(a)$ times. We denote by $A^\sharp$ the set of all multisets on A.

We write $\emptyset$ for the *empty multiset* on A, i.e., the constant function $\emptyset\colon A \to \mathbb{N}$ equal to 0. Given two multisets μ and ν on A, their *union* or *sum* is the multiset $\mu \sqcup \nu$ on A such that $(\mu \sqcup \nu)(a) = \mu(a) + \nu(a)$ for every element $a \in A$. The operation $\sqcup$ equips $A^\sharp$ with a structure of commutative monoid, with $\emptyset$ as neutral element, which characterizes multisets over A. Given an element $a \in A$, we often write $\{a\}$ for the multiset with a as only element. Given two multisets μ and ν, we say that μ is *included* in ν, what we write $\mu \sqsubseteq \nu$ when $\mu(a) \leqslant \nu(a)$ for every $a \in A$. This is the case precisely when there is a multiset μ' such that $\mu \sqcup \mu' = \nu$. This relation makes $A^\sharp$ into a poset which is well-founded.

A partial order $\leqslant$ on a set A induces an order $\leqslant^\sharp$ on $A^\sharp$, called its *multiset extension*, defined by $\mu \leqslant^\sharp \nu$ if and only if

$$\forall b \in A, \qquad \mu(b) > \nu(b) \quad \text{implies} \quad \exists a \in A, \quad a > b \text{ and } \mu(a) < \nu(a).$$

Let us spell it out: for μ to be smaller than ν, it is fine to have more b's as long as ν has more of something greater than b. The following result is due to Dershowitz and Manna [112]:

1.4.2 Proposition. *Given a well-founded poset* $(A, \leqslant)$*, its multiset extension* $(A^\sharp, \leqslant^\sharp)$ *is also well-founded.*

1.4.3 Labeled 1-polygraphs. A *labeled* 1*-polygraph* $(P, \mathcal{L}, \leqslant, \ell)$ consists of

— a 1-polygraph P,
— a set $\mathcal{L}$ of *labels* equipped with a well-founded ordering $\leqslant$, and
— a function $\ell\colon P_1 \to \mathcal{L}$ associating a label to each rewriting step.

1.4.4 Lexicographic maximum measure. Let $(P, \mathcal{L}, \leqslant, \ell)$ be a fixed labeled 1-polygraph. We write $\mathcal{L}^*$ for the sets of words over $\mathcal{L}$, i.e., finite sequences of elements of $\mathcal{L}$. The empty word is noted 1, and the concatenation of two words w and w is noted ww': these operations equip the sets of words with a structure of monoid. Following [350, Definition 3.1], we define the *lexicographic maximum measure* $\|w\|$ of a word $w \in \mathcal{L}^*$ as the multiset defined inductively by

$$\|1\| = \emptyset, \qquad\qquad \|lw\| = \{l\} \sqcup \|w^{\nless l}\|.$$

Above, $w^{\nless l}$ is the subword of w whose letters are not strictly below l, which is formally defined by induction by

$$1^{\nless l} = 1, \qquad\qquad (aw)^{\nless l} = \begin{cases} w^{\nless l} & \text{if } a < l, \\ aw^{\nless l} & \text{otherwise.} \end{cases}$$

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

Informally, the multiset $\|w\|$ thus consists of the letters of w which are not dominated by some letter on their left.

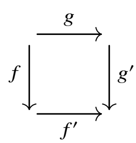
The measure $\|\cdot\|$ is extended to the set of finite rewriting paths of P by setting, for every rewriting path $a_1 \ldots a_n$,

$$\|a_1 \ldots a_n\| = \|\ell(a_1) \ldots \ell(a_n)\|,$$

where $\ell(a_1) \ldots \ell(a_n)$ is the product in the monoid $\mathcal{L}^*$. Finally, the measure $\|\cdot\|$ is extended to the set of finite branchings (a, b) of P, by setting

$$\|(a, b)\| = \|a\| \sqcup \|b\|.$$

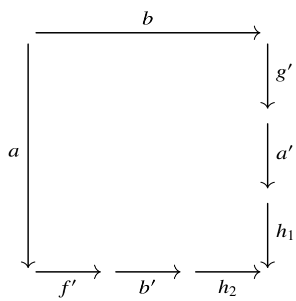
1.4.5 Decreasing diagrams. A diagram of rewriting paths of the form



is *decreasing* if

$$\|ff'\| \leqslant^{\sharp} \|f\| \sqcup \|g\| \qquad \text{and} \qquad \|gg'\| \leqslant^{\sharp} \|f\| \sqcup \|g\|.$$

In the case where $f = a$ and $g = b$ are both 1-generators, it can be shown that the diagram is decreasing if and only if it is of the form



(1.4)

where

— $l < \ell(a)$ for every label l of a rewriting step in f',
— $l < \ell(b)$ for every label l of a rewriting step in g',
— a' is either an identity or a rewriting step labeled by $\ell(a)$,
— b' is either an identity or a rewriting step labeled by $\ell(b)$, and
— $l < \ell(a)$ or $l < \ell(b)$ for every label l of a transition in h_1 (resp. in h_2).

A labeled 1-polygraph is *locally decreasing* when every local branching (a, b) can be completed as a locally decreasing diagram (1.4). We can now recall

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press

van Oostrom's theorem [350, Theorem 3.7], whose proof follows the one of Newman's Lemma 1.3.21:

1.4.6 Theorem. *A locally decreasing* 1*-polygraph is confluent.*

This method is complete, in the sense that given a 1-polygraph with countably many 0-cells which is confluent, there is always a way to choose a well-founded poset $\mathcal{L}$ of labels so that the polygraph is locally decreasing [342, Theorem 14.2.32]. Moreover, we can always choose the set $\mathcal{L} = \{0, 1\}$ with $0 < 1$ as a set of labels, see [122].

https://doi.org/10.1017/9781009498968.003 Published online by Cambridge University Press