Title

Cyrille Chenavier[1] and Maxime Lucas[2]

[1] Inria Lille - Nord Europe, équipe Valse
cyrille.chenavier@inria.fr
[2] Inria Rennes - Bretagne Atlantique, équipe Gallinette
maxime.lucas@inria.fr

Abstract

1 Introduction

2 Well-formed rewriting steps

We fix a commutative field $\mathbb{K}$ as well as a well-founded ordered set $(X, <)$. We denote by $\mathbb{K}X$ the vector space spanned by X: an element $v \in \mathbb{K}X$ is a finite formal linear combination of elements of X with coefficients in $\mathbb{K}$. In particular, for every $v \in \mathbb{K}X$, there exists a unique finite set $\operatorname{supp}(v) \subset X$, called the *support* of v, such that

$$v = \sum_{x \in \operatorname{supp}(v)} \lambda_x x \text{ and } x \in \operatorname{supp}(v) \Rightarrow \lambda_x \neq 0. \tag{1}$$

We denote by $\operatorname{supp}(v)^c = X \setminus \operatorname{supp}(v)$. The sum of $u = \sum \lambda_x x$ and $v = \sum \mu_x x$ equals $\sum (\lambda_x + \mu_x) x$ and the product of $\lambda \in \mathbb{K}$ by v equals $\sum (\lambda \lambda_x) x$. We extend the order $<$ into the multiset order, still written $<$, on $\mathbb{K}X$: we have $u < v$ if for every $x \in \operatorname{supp}(u) \cap \operatorname{supp}(v)^c$, there exists $y \in \operatorname{supp}(v) \cap \operatorname{supp}(u)^c$ such that $y > x$.

We fix a set $R \subseteq X \times \mathbb{K}X$ which represents rewrite rules of the form $x \underset{R}{\longrightarrow} r$. The set R induces the rewriting relation on $\mathbb{K}X$, still written $\underset{R}{\longrightarrow}$, defined as follows:

$$\sum \lambda_x x + v \underset{R}{\longrightarrow} \sum \lambda_x r_x + v, \tag{2}$$

whenever $\lambda_x \neq 0$, $x \underset{R}{\longrightarrow} r_x \in R$ and $x \notin \operatorname{supp}(v)$.

Definition 2.1. A *local strategy* for R is the choice, for every $x \in X$ not minimal for $<$, of a rewriting rule $h_x = x \underset{R}{\longrightarrow} r_x$ such that $r_x < x$.

Suppose chosen such a local strategy h. Any vector v can be decomposed in a unique way as $\sum \lambda_x x + v'$, where $y \in \operatorname{supp}(v')$ implies that y is minimal for $<$, and $x \in \operatorname{supp}(v) \cap \operatorname{supp}(v')^c$ is not. We define a rewriting relation $\underset{h}{\longrightarrow}$ as follows:

$$\sum \lambda_x x + v' \underset{h}{\longrightarrow} \sum \lambda_x r_x + v', \tag{3}$$

where for every x, $h_x = x \underset{R}{\longrightarrow} r_x$.

Definition 2.2. A vector v is said to be a *h-normal form* if it is a normal form for $\xrightarrow[h]{}$.

Example 2.3. Let $X = \{x, y, z, t\}$, $x \xrightarrow[R]{} y$, $y \xrightarrow[R]{} z + t$, $z \xrightarrow[R]{} y - t$. Note that this is not terminating since we have the infinite loop $y \xrightarrow[R]{} z + t \xrightarrow[R]{} (y - t) + t = y$. We choose the order $x > y > z$, and the following distinguished rewrite rules: $h_x = x \xrightarrow[h]{} y$, $h_y = y \xrightarrow[h]{} z + t$. Then the R-normal forms are the $\lambda_t t$, while the h-normal form are all the $\lambda_t t + \lambda_z z$.

Lemma 2.4. *Let v be a vector in $\mathbb{K}X$. Either v is minimal for $<$, or there exists $v' < v$ such that $v \xrightarrow[h]{} v'$. In particular, h-normal forms are precisely the minimal elements of $\mathbb{K}X$ for $<$.*

For each $v \in \mathbb{K}X$, there exists at most one v' such that $v \xrightarrow[h]{} v'$, and $\xrightarrow[h]{}$ is compatible with the termination order $<$. As a consequence, any $v \in \mathbb{K}X$ is sent by multiple applications of $\xrightarrow[h]{}$ to a unique h-normal form that we denote by $H(v)$. This defines a map $H : \mathbb{K}X \to \mathbb{K}X$.

Proposition 2.5. *The map H is a linear projector.*

Proof. The h-normal forms are closed under sums, so that $H(H(v)) = H(v)$ for every v, that is H is a projector. Moreover, if $u \xrightarrow[h]{} u'$ and $v \xrightarrow[h]{} v'$, then we have $u + v \xrightarrow[h]{} u' + v'$. Iterating $\xrightarrow[h]{}$, we get $H(u + v) = H(H(u) + H(v)) = H(u) + H(v)$. $\square$

3 A confluence criterion

Definition 3.1. We say that R is *h-confluent* if for every rewrite rule $x \xrightarrow[R]{} v \in R$, we have $x - v \in \ker(H)$.

Example 3.2. Let us take the same example as in 2.3. Then $H(x) = H(y) = z + t$, with $H(z) = z = H(y - t)$, and so R is h-confluent. Replacing the rule $z \xrightarrow[R]{} y - t$ by $z \xrightarrow[R]{} y$, we get $H(z) = z$ and $H(y) = z + t$, so R is not h-confluent anymore.

Proposition 3.3. *If R is h-confluent, then $u \xleftrightarrow[R]{*} v$ if and only if $u - v \in \ker(H)$.*

Proof. The relation $\xleftrightarrow[R]{*}$ is the closure of $\xrightarrow[R]{}$ under transitivity, symmetry and sum. Since the relation $u - v \in \ker(H)$ is closed under these operations, we get one implication.

Reciprocally, if $u - v \in \ker(H)$ then by definition of H we have $u \xleftrightarrow[h]{*} v$, and in particular $u \xleftrightarrow[R]{*} v$. $\square$

Proposition 3.4. *If R is h-confluent, then $\xrightarrow[R]{}$ is confluent.*

Proof. Let $v,\ v_1,\ v_2 \in \mathbb{K}X$ be such that $v \xrightarrow[R]{*} v_i$, for $i = 1,\ 2$. From Proposition 3.3, $v_1 - v_2$ belongs to $\ker(H)$, that is $H(v_1) = H(v_2)$. Hence, we get

$$\begin{tikzcd}
 & v_1 \arrow[dr, bend left, "*"] & \\
v \arrow[ur, bend left, "*"] \arrow[dr, bend right, "*"'] & & H(v_i) \\
 & v_2 \arrow[ur, bend right, "*"'] &
\end{tikzcd}$$

$\square$

In Theorem 3.6, we introduce a confluence criterion when R satisfies 3.1. For that, we assume that R is equipped with a well-founded order $\prec$ satisfying the following decreasingness property:

Definition 3.5. We say that R is *locally h-confluent* if for every non minimal $x \in X$ and $r = x \xrightarrow[R]{} v$, then letting $h_x = x \xrightarrow[h]{} r_x$, we have the confluence diagram:

$$\begin{tikzcd} & r_x \arrow[dr, dotted, "*"] & \\ x \arrow[ur, bend left, "h_x"] \arrow[dr, bend right, "r"'] & & v' \\ & v \arrow[ur, dotted, "*"'] & \end{tikzcd}$$

where each rewriting step occurring in the dotted arrows are strictly smaller than r for $\prec$.

Theorem 3.6. *If R is locally h-confluent, then R is h-confluent. In particular, $\xrightarrow[R]{}$ is confluent.*

Proof. We reason by induction on r. Looking at the square corresponding to r:

$$\begin{tikzcd} & r_x \arrow[dr, dotted, "*"] & \\ x \arrow[ur, bend left, "h_x"] \arrow[dr, bend right, "r"'] & & v' \\ & v \arrow[ur, dotted, "*"'] & \end{tikzcd}$$

We have $H(x) = H(r_x)$ by definition of H, and $H(r_x) = H(v') = H(v)$ by induction hypothesis, which concludes the proof. $\square$

Let us show how the diamond Lemma fits as a particular case of our set up.

Theorem 3.7 ([1])**.** *Assume that $\xrightarrow[R]{}$ is terminating and that for every $x \in X$, $x \xrightarrow[R]{} r$ and $x \xrightarrow[R]{} r' \in R$, r and r' are joingable. Then, $\xrightarrow[R]{}$ is confluent.*

Proof. We define the relation $x > y$ on X whenever $x \xrightarrow[R]{} v$ exists such that $y \in \mathrm{supp}(v)$. The induced order relation is well-founded. By definition, if $x \in X$ is not minimal for $>$, then x is not an R-normal form. Let us fix an arbitrary rewriting step $h_x = x \xrightarrow[h]{} r_x$. By definition of $>$, $r_x < x$ so that h is a local strategy. Ordering the rewrite rules by their left hand sides makes R locally h-confluent. Theorem 3.6 finally shows that R is confluent. $\square$

References

[1] George M. Bergman. The diamond lemma for ring theory. *Adv. in Math.*, 29(2):178–218, 1978.