Revisiting Term-Rewriting in Algebra

William Sit[1]
The City College of The City University of New York

Kolchin Seminar in Differential Algebra
February 13, 2015 (Graduate Center, CUNY)

[1]Preliminary report based on joint work with Li Guo, Rutgers University at Newark; Ronghua Zhang, Yunnan University, Kunming, China; Xing Gao and Shanghua Zheng, Lanzhou University, China.

Outline

- Basics of Abstract Rewriting Systems
- General Term-Rewriting Systems
- Rewriting for Basis of Free Modules
- Simple Term Rewriting Systems
- Hierarchy of Binary Relations in Rewriting
- Lemma and Main Theorem on Confluence
- Locally Base-Confluence
- Extending to Rewriting in Operated Algebras
- Ideas on Termination

Symbolic Computation in Algebra

- Let **k** be a commutative unitary ring. An **algebra** in this talk means an associative **k**-algebra that is free as a **k**-module, but it need not be commutative or unitary.
- Typical examples are free algebras in a category $\mathcal{C}$, such as that of
  - finitely generated algebra,
  - differential algebra,
  - difference algebra,
  - operated algebra.
- Given a set X of variables, a free algebra over X in $\mathcal{C}$ is the unique (up to isomorphism) initial object in the category whose objects are set maps $X \to A$, where A is an object in $\mathcal{C}$.
- Symbolic computation is based on rewriting systems in these free objects.

What is a Rewriting System?

- An (abstract) **rewriting system** (ARS) is simply a set V together with a binary relation, traditionally denoted by $\to$. A **relation** is just a subset of $V \times V$.
- An ARS is also known as a **reduction system**, or a **state transition system**.
- The binary relation is understood as performing some action that changes one element to another; the action may be called "rewriting", "reducing", or "transforming" an element a to b if $a \to b$ (or a state a being transited to another state b).
- A **rule** is just a pair (a, b) in the relation: $a \to b$.

Basic Notions for Rewriting Systems

- The **transitive reflexive closure** of $\to$ is denoted by $\overset{*}{\to}$ or $\twoheadrightarrow$. So $a \overset{*}{\to} b$ means there is a finite chain of reductions: $a = a_0 \to a_1 \to \cdots \to a_n = b$ with $n \geqslant 0$.
- An element $a \in V$ is **reducible** if for some $b \in V$, $b \neq a$ and $a \to b$. Otherwise, it is called **irreducible**.
- A **normal form** of a is a b such that b is irreducible, and $a \overset{*}{\to} b$. A normal form for a need not exist nor be unique.
- If every element $a \in V$ has a normal form, we say $\to$ is **normalizing**.
- **terminating** or **noetherian** if there is no infinite chain of reductions $a_0 \to a_1 \to a_2 \cdots$. Terminating implies normalizing.

What Makes a Good ARS for Symbolic Computation?

- Two elements a and b are **joinable** if there is a c such that $a \xrightarrow{*} c$ and $b \xrightarrow{*} c$. This is denoted by $a \downarrow b$.
- A pair of distinct reductions $(a \xrightarrow{*} b_1, a \xrightarrow{*} b_2)$ (resp. $(a \to b_1, a \to b_2)$) is called a **fork** (resp. **local fork**) at a. The fork is **joinable** if $b_1 \downarrow b_2$.
- An ARS is **confluent** (resp. **locally, or weakly, confluent**) if every fork (resp. local fork) is joinable, and
- **convergent** if it is both terminating and confluent. In a normalising and confluent system, every element has a unique normal form.
- **Theorem (Newman's Lemma)**: **A terminating ARS is confluent if and only if it is locally confluent.**

Church-Rosser Property

- The **symmetric closure** of $\rightarrow$ is the relation $a \leftrightarrow b$ defined as "either $a \rightarrow b$ or $b \rightarrow a$."
- The transitive reflexive closure of $\leftrightarrow$ is denoted by $\overset{*}{\longleftrightarrow}$. It is the smallest equivalence relation generated by $\rightarrow$.
- An ARS is said to have the **Church-Rosser property** if for all $a, b \in V$, $a \overset{*}{\longleftrightarrow} b$ implies $a \downarrow b$.
- It is known that CR is equivalent to confluent. Indeed, CR, confluent, and transitivity of $\downarrow$ are all equivalent. In a confluent system, the relations $\overset{*}{\longleftrightarrow}$ and $\downarrow$ are identical.
- Using this, for a confluent system, if $a \overset{*}{\longleftrightarrow} b$, then by CR, $a \downarrow b$ and hence (1) if a and b are both normal forms, then $a = b$ (2) if b is a normal form, then $a \overset{*}{\rightarrow} b$.

Term Algebra

- A **signature** Σ is a set F of function symbols, a set R of relation symbols and an arity function $ar : F \sqcup R \to \mathbb{N}$. Functions symbols with arity 0 are called constants (symbols).
- The signature for abelian groups is abbreviated to $\sigma = (+, -, 0)$ and for a commutative ring, to $\sigma = (+, \cdot, 0, 1)$.
- Let X be a set (of variable symbols, disjoint from the signature). Terms are defined inductively and the **Σ-term-algebra over X** is the smallest set $\mathcal{T}(X)$ satisfying:
  - variables and constant symbols are terms.
  - if f is a function of arity n and $t_1, \ldots, t_n$ are terms, then $f(t_1, \ldots, t_n)$ is a term.
- In computation, terms are syntactic objects representable by trees when parsed.
- $\mathcal{T}(X)$ is a freely generated algebraic structure over the function symbols of Σ and X.

Term Rewriting Systems in Algebras

- More general settings are based on many-sorted logic. For example, modules over a ring is a two-sorted structure because two sorts of algebraic structures are intermingled.
- A **term-rewriting system** is a set of **term-rewriting rules**, which are pairs of terms (ℓ, r), written as $\ell \to r$. The rule is applied to a term s if some subterm of s matches ℓ at some position, in which case, s can be rewritten by substituting that occurrence of ℓ by r resulting in another term t. The rule $\ell \to r$ thus generates many more (abstract) rewriting rules $s \to t$ on the term-algebra.
- Rewriting rules are typically based on interpretations of the relation symbols R. The rewriting rules and term algebra over X are used to provide models free over X.

Free Modules with Given Basis

- Let V be a free $\mathbf{k}$-module with a given $\mathbf{k}$-basis W.
- For $f \in V$, the **support** or **W-support** $\mathrm{Supp}(f) = \mathrm{Supp}_W(f)$ of f is the set consisting of $w \in W$ appearing in f (with non-zero coefficients), when f is expressed as a unique linear combination of $w \in W$ with coefficients in $\mathbf{k}$.
- Let $f, g \in V$. We use $f \dot{+} g$ to indicate the relation that $\mathrm{Supp}(f) \cap \mathrm{Supp}(g) = \emptyset$. If this is the case, we say $f + g$ is a **direct sum** of f and g, and by abuse, we use $f \dot{+} g$ also for the sum $f + g$.
- Note $\mathrm{Supp}(0) = \emptyset$ and hence $f \dot{+} 0$ for any $f \in V$.

ARS to TRS, From Set to Linear Algebra

- A **rewriting system $\to$ on a free k-module V relative to a fixed basis W** is a binary relation (as a subset Π) of $W \times V$.
- The image $\pi_1(\Pi)$ of Π under the first projection map $\pi_1 : W \times V \to W$ will be denoted by T.
- We extend $\to$ to a term-rewriting system $\to_\Pi$ on V by linearity.
- Let the coefficient of w in $f \in V$ be c_w. We define the **w-complement of f** to be $R_w(f) := f - c_w w \in V$, so that $f = c_w w \dot{+} R_w(f)$.
- For $t \in \mathrm{Supp}(f) \cap T$ and $t \to v$, we view this as a term-rewriting rule on V, that is, we may replace t in f by v, resulting in a new element $g := c_t v + R_t(f) \in V$ and say f **reduces to**, or **rewrites to, g in one-step**; notation: $f \to_\Pi g$, or in more detail, by $f \xrightarrow{(t,v)}_\Pi g$.

Simpe Term-Rewriting Systems

- We say the rewriting system $\to$ is **simple** if $t \dot{+} v$ for all $t \to v$.
- Example: Let $W = \{x, y\}$. Then $\Pi = \{x \to y, y \to x\}$ is simple. Every element is reducible, none has a normal form, and Π is neither normalizing nor terminating, but is confluent.
- Example: Let $W_1 = \{xy, x, y\}$, $W_2 = \{xy - x - y, x, y\}$. Let $\Pi_1 = \{xy \to x + y\}$, $\Pi_{12} = \{x \to y\}$, and $\Pi_2 = \{xy - x - y \to 0\}$. Let $f := xy$, $g = xy - x + y$.
  - These are simple term-rewriting systems: Π_1 w.r.t W_1, Π_{12} w.r.t. both W_1 and W_2, and Π_2 w.r.t. W_2.
  - f is Π_1-reducible to $x + y$ (W_1).
  - f is Π_2-reducible to $x + y$ (W_2).
  - f is Π_{12}-irreducible (W_1).
  - f is Π_{12}-reducible to g (W_2)—normal form.
  - g is Π_1-reducible to $2y$ (W_1), Π_2-reducible to $2y$ (W_2).
  - g is Π_{12}-reducible to $xy - 2y$ (W_1).

A Hierarchy Lemma for Simple TRS

Lemma: Let V be a free $\mathbf{k}$-module with a $\mathbf{k}$-basis W and let Π be a term-rewriting system on V relative to W. For any $f, g \in V$, consider the following properties:

(1). $f \to_\Pi g$;

(2). $(f - g) \to_\Pi 0$;

(3). $(f - g) \overset{*}{\to}_\Pi 0$; (equivalently, $(f - g) \downarrow_\Pi 0$);

(4). $f \downarrow_\Pi g$;

Then (1) $\implies$ (4), (2) $\implies$ (3) $\implies$ (4), and if Π is simple, also (1) $\implies$ (2). None of the reverse implications holds.

Examples

- Let V be the $\mathbf{k}$-submodule generated by $W = \{xy, x, y\}$ of the polynomial ring $\mathbf{k}[x, y]$ in two indeterminates x, y. Let $\Pi := \{xy \to x\}$. Then Π is simple and $T = \{xy\}$. Let $f = 2xy + y$, $g = xy + x + y$. Then $f - g = xy - x \to_\Pi 0$ (2), but $f \to_\Pi 2x + y$, which is irreducible and $\neq g$, showing that (2) does not imply (1). Moreover, $f \downarrow_\Pi g$ (4) since $g \to 2x + y$, showing that (4) does not imply (1).
- $\Pi := \{xy \to x, xy \to y\}$ is simple. The two polynomials $f := xy + x$ and $g := xy + y$ are joinable since $f \xrightarrow{(xy,y)}_\Pi y + x$ and $g \xrightarrow{(xy,x)}_\Pi y + x$. However, $f - g = x - y$ is irreducible and non-zero, showing that (4) does not imply (3).
- As will be known later, if (4) does imply (3) for all $f, g \in V$, then Π is confluent.

Another Example

- Let V be the $\mathbf{k}$-submodule generated by $W = \{xy, x, y, z\}$ of the polynomial ring $\mathbf{k}[x, y, z]$ in three indeterminates x, y, z and let

$$\Pi := \{xy \to x, xy \to y, xy \to z\},$$

  which is simple. Then $T = \{xy\}$ and the polynomials $f := xy + x$ and $g := xy + z$ are joinable to $g_1 := x + z$, and the polynomials g and $h := xy + y$ are joinable to $g_2 := y + z$. However f and h are also joinable (to $x + y$) *without* necessarily g_1, g_2 (which are irreducible) being joinable.

- As already shown for any rewriting system, confluence is equivalent to the transitivity of $\downarrow_\Pi$.

A Lemma before Main Theorem

Let V be a free k-module with a k-basis W and let Π be a simple term-rewriting system on V relative to W. Let $f, g, h \in V$. If $f \to_\Pi g$, then $(f + h) \downarrow_\Pi (g + h)$.

Proof. By Definition, there exist $t \to v$ and $0 \neq c \in \mathbf{k}$ such that $f = ct \dot{+} R_t(f)$ and $g = cv + R_t(f)$. Let $h = bt \dot{+} R_t(h)$, where $b \in \mathbf{k}$ (b may be zero). Since Π is simple, we have $t \dot{+} v$. Since $t \dot{+} R_t(f)$, we have $t \dot{+} g$ and

$$\begin{aligned} g + h = bt \dot{+} (g + R_t(h)) &\overset{*}{\to}_\Pi bv + (g + R_t(h)) \\ &= (b + c)v + R_t(f) + R_t(h). \end{aligned}$$

On the other hand, we also have

$$\begin{aligned} f + h &= (b + c)t \dot{+} (R_t(f) + R_t(h)) \\ &\overset{*}{\to}_\Pi (b + c)v + R_t(f) + R_t(h). \end{aligned}$$

Thus $(f + h) \downarrow_\Pi (g + h)$.

Main Theorem on Confluence

Let V be a free $\mathbf{k}$-module with a $\mathbf{k}$-basis W and let Π be a simple term-rewriting system on V relative to W. **The following properties on Π are equivalent.**

(a). $\to_\Pi$ is confluent, that is, for any $f, g, h \in V$, **confluence**

$$(f \overset{*}{\to}_\Pi g,\ f \overset{*}{\to}_\Pi h) \implies g \downarrow_\Pi h.$$

(b). For all $f, g, h \in V$, **transitivity of $\downarrow_\Pi$**

$$f \downarrow_\Pi g,\ g \downarrow_\Pi h \implies f \downarrow_\Pi h.$$

(c). For all $f, g, f', g' \in V$, **2-additivity of $\downarrow_\Pi$**

$$f \downarrow_\Pi g,\ f' \downarrow_\Pi g' \implies (f + f') \downarrow_\Pi (g + g').$$

Theorem Continued

(d). For all $r \geqslant 1$ and $f_1, \ldots, f_r, g_1, \ldots, g_r \in V$,

n-additivity of $\downarrow_\Pi$

$$f_i \downarrow_\Pi g_i \quad (1 \leqslant i \leqslant r) \implies \left(\sum_{i=1}^{r} f_i\right) \downarrow_\Pi \left(\sum_{i=1}^{r} g_i\right).$$

(e). For all $f, g, h' \in V$, **1-additivity of $\downarrow_\Pi$**

$$f \downarrow_\Pi g \implies (f + h') \downarrow_\Pi (g + h').$$

(f). For all $f, g \in V$, **1-transposition of $\downarrow_\Pi$**

$$f \downarrow_\Pi g \implies (f - g) \xrightarrow{*}_\Pi 0 \quad (\text{that is}, (f - g) \downarrow_\Pi 0).$$

(g). For all $r \geqslant 1$ and $f_1, \ldots, f_r, g_1, \ldots, g_r \in V$,

n-transposition of $\downarrow_\Pi$

$$f_i \downarrow_\Pi g_i \quad (1 \leqslant i \leqslant r) \implies \left(\sum_{i=1}^{r} f_i\right) - \left(\sum_{i=1}^{r} g_i\right) \xrightarrow{*}_\Pi 0.$$

Main Theorem Continued

(h). For all $r \geqslant 1$ and $f_1, \ldots, f_r, g_1, \ldots, g_r \in V$,

zero-sum of $\downarrow_\Pi$

$$f_i \downarrow_\Pi g_i \quad (1 \leqslant i \leqslant r) \text{ and } \sum_{i=1}^{r} g_i = 0 \implies \left(\sum_{i=1}^{r} f_i\right) \xrightarrow{*}_\Pi 0.$$

(i). For all $r \geqslant 1$ and $f_1, \ldots, f_r, g_1, \ldots, g_r \in V$,

***n*-transpose of $\xrightarrow{*}_\Pi$**

$$f_i \xrightarrow{*}_\Pi g_i \quad (1 \leqslant i \leqslant r) \implies \left(\sum_{i=1}^{r} f_i\right) - \left(\sum_{i=1}^{r} g_i\right) \xrightarrow{*}_\Pi 0.$$

(j). For all $r \geqslant 1$ and $f_1, \ldots, f_r, g_1, \ldots, g_r \in V$,

zero-sum of $\xrightarrow{*}_\Pi$

$$f_i \xrightarrow{*}_\Pi g_i \quad (1 \leqslant i \leqslant r), \text{ and } \sum_{i=1}^{r} g_i = 0 \implies \left(\sum_{i=1}^{r} f_i\right) \xrightarrow{*}_\Pi 0.$$

Main Theorem Continued

(k). For all $r \geqslant 1$ and $f_1, \ldots, f_r \in V$, **zero-additivity of $\xrightarrow{*}_\Pi$**

$$f_i \xrightarrow{*}_\Pi 0 \quad (1 \leqslant i \leqslant r) \implies \left(\sum_{i=1}^{r} f_i \right) \xrightarrow{*}_\Pi 0.$$

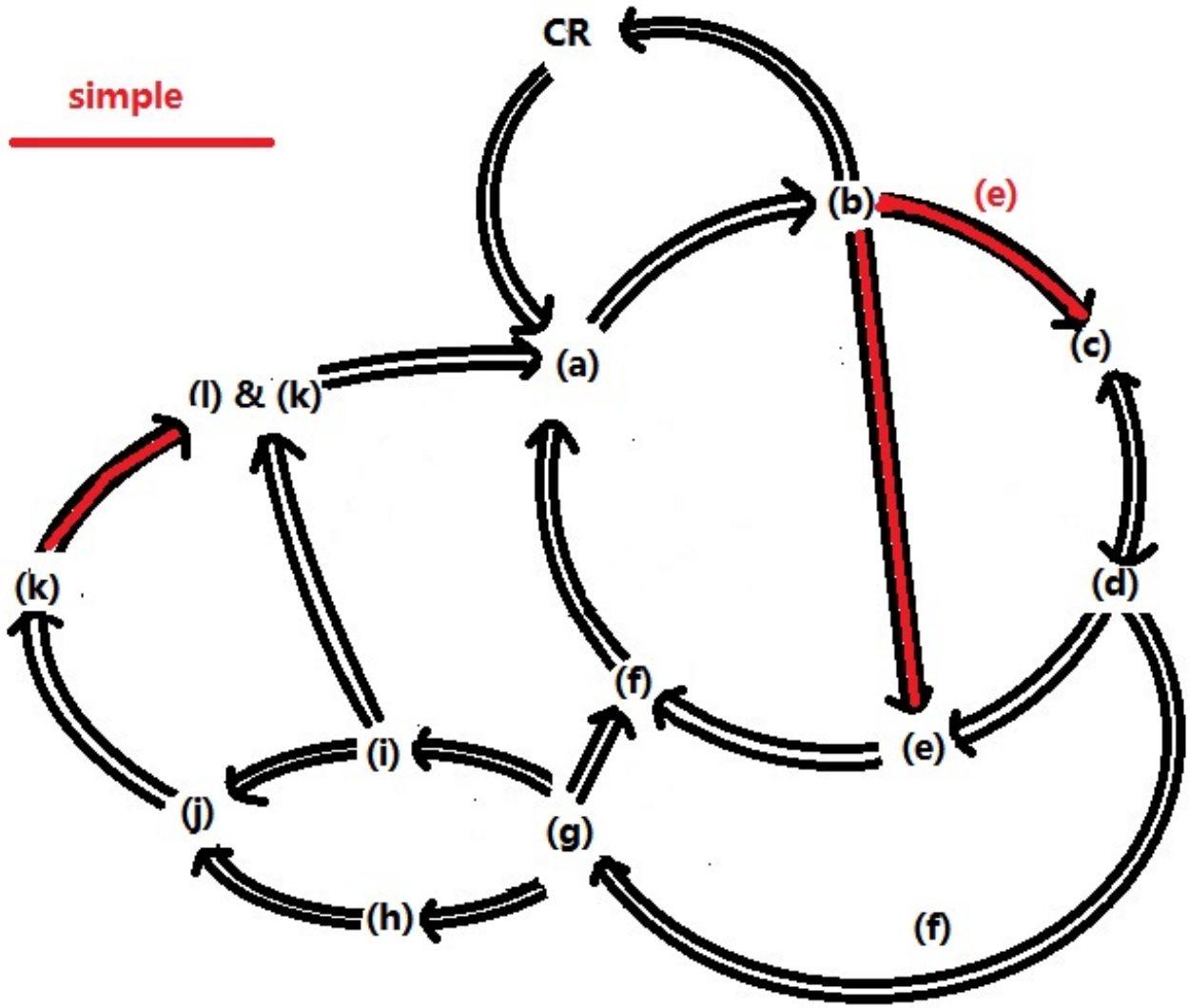
When any of the above holds, we also have

(l). For all $f, g \in V$, **transposition of $\xrightarrow{*}_\Pi$**

$$f \xrightarrow{*}_\Pi g \implies f - g \xrightarrow{*}_\Pi 0.$$

.

Proof Steps



A Trivial Example

- The Lemma (let alone the stronger property (ℓ)) need not hold if Π is not simple, even when $\to_\Pi$ is confluent.
- **Example**: Let V be the free-$\mathbf{k}$-submodule generated by $W = \{t, v\}$ in the polynomial ring $\mathbf{k}[t, v]$. Let $\Pi = \{t \to t + v\}$. Then Π is confluent but not simple. (ℓ) is false since $t \overset{*}{\to}_\Pi t + v$ but $0 \downarrow_\Pi v$ does not hold.
- To see that $\to_\Pi$ is confluent, note that any reduction chain for $f = at + bv$ (with $a, b \in \mathbf{k}$) must end with some $g_m = at + (ma + b)v$ for some natural number m. Thus a fork at f ends at some g_m and g_n. If $m \geqslant n$, then by applying $m - n$ reductions to g_n, $g_n \overset{*}{\to}_\Pi g_m$ and hence the two are joinable.

Another Trivial Example

- The failure of property (ℓ) may be used to show $\to_\Pi$ is not confluent.
- **Example**: Let V be the free-$\mathbf{k}$-submodule generated by $W = \{t, u, v\}$ in the polynomial ring $\mathbf{k}[t, u, v]$. Let $\Pi = \{t \to u, u \to t + v\}$. Then Π is simple and since Property (ℓ) does not hold for $t \overset{*}{\to}_\Pi t + v$, $\to_\Pi$ is not confluent. Is the fork $(t + u \overset{(t,u)}{\to}_\Pi 2u, t + u \overset{(u,t+v)}{\to}_\Pi 2t + v \overset{(t,u)}{\to}_\Pi 2u + v)$ joinable?
- The proof of the Theorem shows that none of $(c), (d), (g), (i)$ need hold when Π is confluent but not simple, or when Π is simple but not confluent, since these imply (ℓ) even when Π is neither simple nor confluent. These properties (including $(e), (f)$) are each strictly stronger than confluence.

Some More Equivalences and Remarks

- By an induction, each of the properties (g), (h), (i), (j), and (k) is also equivalent to confluence when "For all $r \geqslant 1$" is replaced by "For $r = 2$".
- For a simple term-rewriting system Π with $\to_\Pi$ confluent, the relation $f \downarrow_\Pi g$ is transitive, additive, terms on either side are freely transposable, and $f \downarrow_\Pi g$ is interchangeable with $f - g \overset{*}{\to}_\Pi 0$.
- The property $f \overset{*}{\to}_\Pi 0$ for $f \in V$ is additive, yet for the relation $\overset{*}{\to}_\Pi$, only the *entire* right-hand side may be transposed.
- The property (ℓ) is just (i) when $r = 1$. However, unlike property (f), which is (g) when $r = 1$, property (ℓ) does not imply confluence.

Two Notions of Distance

- Suppose $f, g \in V$ are joinable. The **joinable distance** $d_\Pi^\vee(f, g)$ **between** f **and** g is the minimum of $m + n$ over all possible p and reductions to p:

$$f \xrightarrow{m}_\Pi p, \;\; g \xrightarrow{n}_\Pi p, \;\; m \geqslant 0, \;\; \text{and} \;\; n \geqslant 0.$$

If $m, n \in \mathbb{N}$ are such that $m + n = d$, then by minimality there exist distinct $f_0, f_1, \ldots, f_m \in V$ and distinct $g_0, g_1, \ldots, g_n \in V$ with $f_m = g_n$ and

$$f = f_0 \to_\Pi f_1 \to_\Pi \cdots \to_\Pi f_m, \quad g = g_0 \to_\Pi g_1 \to_\Pi \cdots \to_\Pi g_n.$$

- If $(f \xrightarrow{*}_\Pi g_1, f \xrightarrow{*}_\Pi g_2)$ is a fork, we define the **fork distance** $d_\Pi^\wedge(f, g_1, g_2)$ **between** f **and** g_1, g_2 to be the minimum of $m + n$ over all reductions $f \xrightarrow{m}_\Pi g_1$ and $f \xrightarrow{n}_\Pi g_2$, $(m \geqslant 0, n \geqslant 0)$.

Transitivity $\Longrightarrow$ 1-Additivity of $\downarrow_\Pi$

Since $f, g \in V$ are joinable, let $d = d^\vee_\Pi(f, g)$ and $m + n = d$ as above. If $d = 0$, then $f = g$ and clearly $(f + h') \downarrow_\Pi (g + h')$. If $d = 1$, then either $f \to_\Pi g$ or $g \to_\Pi f$ and these cases follow from the Lemma. Suppose now $d = s + 1$ where $s \geqslant 1$, and suppose by induction that for all $\overline{f}, \overline{g} \in V$,

$$\overline{f} \downarrow_\Pi \overline{g},\ d^\vee_\Pi(\overline{f}, \overline{g}) \leqslant s \implies (\overline{f} + h') \downarrow_\Pi (\overline{g} + h').$$

Since $d \geqslant 2$, either $m \geqslant 1$ or $n \geqslant 1$ (or both). Without loss of generality, we assume $m \geqslant 1$. Then $f_1 \downarrow_\Pi g$ and $d^\vee_\Pi(f_1, g) \leqslant s$. By the induction hypothesis, $(f_1 + h') \downarrow_\Pi (g + h')$. It follows by the Lemma that $(f + h') \downarrow_\Pi (f_1 + h')$, and by the transitivity assumption that $(f + h') \downarrow_\Pi (g + h')$. This completes the induction.

Local Base-Forks and Local Base-Confluence

- A **local base-fork** is a fork $(ct \to_\Pi cv_1, ct \to_\Pi cv_2)$ where $t \to v_1, t \to v_2$ and $c \in \mathbf{k}$, $c \neq 0$. The rewriting system Π is **locally base-confluent** if for every local base-fork $(ct \to_\Pi cv_1, ct \to_\Pi cv_2)$, we have $c(v_1 - v_2) \overset{*}{\to}_\Pi 0$.
- Example. Let V be the free $\mathbf{k}$-submodule of the polynomial ring $\mathbf{k}[x, y, z, u, v]$ with a $\mathbf{k}$-basis $W = \{xyz, x, y, z, u, v\}$. Let Π consist of 6 rules:

$$\begin{aligned} xyz &\to x + v, & x &\to u, \\ xyz &\to y, & y &\to u + v, \\ xyz &\to z + u, & z &\to v. \end{aligned}$$

Then $T = \{xyz, x, y, z\}$ and Π is a simple term-rewriting system. The only local base-forks start at xyz; and Π is locally base-confluent (in particular, the local base-forks are all joinable to $u + v$).

Example Continued

- Now consider the three polynomials in V:

$$f = xyz + x, \quad g = xyz + y - v, \quad h = xyz + z + u - v.$$

Then we have two joinable pairs:

$$(f \overset{(xyz,\, y)}{\longrightarrow}_{\Pi} x + y \quad , \quad g \overset{(xyz,\, x+v)}{\longrightarrow}_{\Pi} x + y),$$
$$(g \overset{(xyz,\, z+u)}{\longrightarrow}_{\Pi} y + z + u - v \quad , \quad h \overset{(xyz,\, y)}{\longrightarrow}_{\Pi} y + z + u - v).$$

Thus $f \downarrow_{\Pi} g$ and $g \downarrow_{\Pi} h$. However, while we have $f \downarrow_{\Pi} h$ because $(x + y) \overset{(x,u)}{\longrightarrow}_{\Pi} (u + y)$ and $(y + z + u - v) \overset{(z,v)}{\longrightarrow}_{\Pi} (u + y)$, the joinability of $x + y$ and $y + z + u - v$ does not come directly from the joinability of the local base-forks, which all join to $u + v$, not $u + y$.

Linear Order on Reducible Terms

- Let T be the set of reducible terms under Π. A partial order $\preccurlyeq$ (or its corresponding strict partial order $\prec$) on T is **compatible with Π** if for all $(t, v) \in \Pi$, we have $t' \prec t$ for any $t' \in \mathrm{Supp}(v) \cap T$ (we shall abbreviate this property of (t, v) by $v \prec t$ or $t \succ v$). A necessary condition that such an order exists is that Π is simple.
- Let $\preccurlyeq$ be a linear order on T and let $f \in V$. The **reducible leader** of f, denoted by $L(f)$, or $L_{\preccurlyeq}(f)$ or $L_{\Pi,\preccurlyeq}(f)$ if necessary, is the unique maximum $t \in \mathrm{Supp}(f) \cap T$.
- **Lemma**: Let $\preccurlyeq$ be a linear order on $T = \pi_1(\Pi)$ that is compatible with a simple term-rewriting system Π on a free $\mathbf{k}$-module V with basis W. Let $f, g \in V$ and suppose $f \overset{(t,v)}{\to}_{\Pi} g$ for some $(t, v) \in \Pi$. Then $L(g) \preccurlyeq L(f)$, where equality holds if and only if $L(g) \neq t$.

Proof of Lemma

- We may write $f = (c_1 t_1 + \cdots + c_r t_r) \dot{+} h$ for some integer $r \geqslant 1$, where $\{t_1, \ldots, t_r\} = \mathrm{Supp}(f) \cap T$ with $t_1 \succ \cdots \succ t_r$ (hence $c_1, \ldots, c_r \in \mathbf{k}$ are all non-zero), and h belongs to the $\mathbf{k}$-submodule of V generated by the complement $W \setminus T$ of T in W.

- By Definition, $L(f) = t_1$. Let i be the unique index, $1 \leqslant i \leqslant r$, such that $t_i = t$. Then

$$\begin{aligned} g &= c_i v + R_t(f) \\ &= c_1 t_1 + \cdots + c_{i-1} t_{i-1} + c_i v + c_{i+1} t_{i+1} + \cdots + c_r t_r + h. \end{aligned}$$

  Now $t_1 \succcurlyeq t_i = t \succ v$ since $\preccurlyeq$ is compatible with Π. Thus $L(g) = t_1 = L(f)$ if $i \neq 1$ and $L(g) \prec t_1$ if $i = 1$.

Locally Base-Confluent implies Locally Confluent

- **Theorem**. Let V be a free $\mathbf{k}$-module with a $\mathbf{k}$-basis W and let Π be a simple term-rewriting system on V. Suppose we have a linear order $\preccurlyeq$ on T compatible with Π. If Π is locally base-confluent, it is locally confluent.

- **Corollary**. If $\rightarrow_\Pi$ is terminating, then it is locally base-confluent if and only if it is confluent, in which case, $\rightarrow_\Pi$ is converging.

- Proof of Corollary. If $\rightarrow_\Pi$ is confluent and $(ct \rightarrow_\Pi cv_1, ct \rightarrow_\Pi cv_2)$ is a local base-fork, then $cv_1 \downarrow_\Pi cv_2$. By Property (f), $cv_1 - cv_2 \stackrel{*}{\rightarrow}_\Pi 0$ and hence Π is locally base-confluent. The converse follows from Newman's Lemma.

Proof of Theorem.

- Suppose Π is locally base-confluent. Let $(g \to_\Pi f, g \to_\Pi h)$ be a local fork in V. Then there exist $(t_1, v_1), (t_2, v_2) \in \Pi$ such that $g \xrightarrow{(t_1,v_1)}_\Pi f$ and $g \xrightarrow{(t_2,v_2)}_\Pi h$.
- To prove $f \downarrow_\Pi h$, first suppose $t_1 \neq t_2$. Without loss of generality, we may suppose $t_1 \succ t_2$.
- Then we may write $g = c_1 t_1 \dot{+} (c_2 t_2 \dot{+} r) = c_2 t_2 \dot{+} (c_1 t_1 \dot{+} r)$ for some $r \in V$, $c_1, c_2 \in \mathbf{k}$ and $c_1 \neq 0$, $c_2 \neq 0$.
- So $f = c_1 v_1 + (c_2 t_2 \dot{+} r)$ and $h = c_2 v_2 + (c_1 t_1 \dot{+} r)$.
- Hence $f - h = c_1(v_1 - t_1) + c_2(t_2 - v_2)$.
- Since $t_1 \succ v_1$ and $t_1 \succ t_2 \succ v_2$, we have $f - h \xrightarrow{(t_1,v_1)}_\Pi c_2(t_2 - v_2) \xrightarrow{(t_2,v_2)}_\Pi 0$.
- Thus we have $f \downarrow_\Pi h$.

Proof of Theorem continued

- Next, we suppose $t_1 = t_2$.
- Let $t := t_1 = t_2$ and $g = ct \dot{+} R_t(g)$ for some $c \in \mathbf{k}$ and $c \neq 0$.
- Then $f = cv_1 + R_t(g)$ and $h = cv_2 + R_t(g)$.
- By hypothesis, the local base-fork $(ct \to_\Pi cv_1, ct \to_\Pi cv_2)$ implies that $f - h = cv_1 - cv_2 \overset{*}{\to}_\Pi 0$. By hierarchy, $f \downarrow_\Pi h$.
- Remark. If we had defined local base-fork by requiring $cv_1 \downarrow_\Pi cv_2$, then we cannot deduce $f - h \overset{*}{\to}_\Pi 0$ from $cv_1 \downarrow_\Pi cv_2$ because we do not necessarily have $cv_1 - cv_2 \overset{*}{\to}_\Pi 0$.

Extending to Other Algebras

- Polynomial Algebra: basis consists of monomials
- Differential Algebra: basis consists of differential monomials
- Rota-Baxter Algebra: basis consists of Rota-Baxter words
- Operated Polynomial Algebra: basis consists of operated monomials

Term-Rewriting Chains

- Let Π be a term-rewriting system (not necessarily simple) on a free $\mathbf{k}$-module V relative to a basis W of V. Let T be the set of Π-reducible terms.

- Let $f, g \in V$. A **term-rewriting chain in Π** (or simply, a **Π-chain**) **from f to g of length m** is a sequence of m term-rewriting steps $f \overset{m}{\to}_{\Pi} g$ explicitly given by

$$C : f = g_0 \overset{(t_0, v_0)}{\longrightarrow}_{\Pi} g_1 \overset{(t_1, v_1)}{\longrightarrow}_{\Pi} g_2 \cdots \overset{(t_i, v_i)}{\longrightarrow}_{\Pi} \cdots g_{m-1} \overset{(t_{m-1}, v_{m-1})}{\longrightarrow}_{\Pi} g_m = g,$$

where $g_0, g_1, \ldots, g_m \in V$, $g_0 = f$, $g_m = g$, and for $0 \leqslant i < m$, $(t_i, v_i) \in \Pi$, and $t_i \in \mathrm{Supp}(g_i) \cap T$.

Descendants

- For any $f \in V$, an element $t' \in T$ is said to be a **descendant of f** if there exist some $g \in V$ and some regular element $b \in \mathbf{k}$, such that $t' \in \mathrm{Supp}(g)$ and $bf \xrightarrow{*}_{\Pi} g$.
- The set of all descendants of f is denoted by $\mathcal{D}_{\Pi}(f)$ or simply by $\mathcal{D}(f)$. Clearly, $\mathcal{D}(f)$ contains $\mathrm{Supp}(f) \cap T$ by definition.
- For any $t' \in \mathcal{D}(f)$, a **descendant chain from f to t'** is a Π-chain from bf to g of some length m for some regular element $b \in \mathbf{k}$, such that $t' \in \mathrm{Supp}(g)$.
- A **minimum descendant chain** is one with the shortest length $\gamma(f, t')$, which is called the **generation index of t' from f** (or **from f to t'**).
- Note that $\gamma(f, t') = 0$ if and only if $t' \in \mathrm{Supp}(f)$.

Some Simple Results

- For any $b \in \mathbf{k}$ and $b \neq 0$, we have $\mathrm{Supp}(bf) \subseteq \mathrm{Supp}(f)$. If furthermore, b is regular, then $\mathrm{Supp}(bf) = \mathrm{Supp}(f)$.

- Let $b \in \mathbf{k}$ be regular and the above be a Π-chain from f to g. Then

$$bf = bg_0 \xrightarrow{(t_0, v_0)}_{\Pi} bg_1 \cdots \xrightarrow{(t_i, v_i)}_{\Pi} \cdots bg_{m-1} \xrightarrow{(t_{m-1}, v_{m-1})}_{\Pi} bg_m = bg$$

  is a Π-chain from bf to bg of length m.

- If $f \xrightarrow{*}_{\Pi} g$, then $\mathcal{D}(g) \subseteq \mathcal{D}(f)$.

A Conjecture

- Let $\mathbf{k}$ be a domain. Let Π be a term-rewriting system (not necessarily simple) on a free $\mathbf{k}$-module V with basis W. Let T be the set of Π-reducible terms. Let $f \in V$ and $t \in \mathrm{Supp}(f) \cap T$.
- Let $t' \in \mathcal{D}(t)$ and $m = \gamma(t, t')$. Let

$$bt = g_0 \overset{(t_0, v_0)}{\longrightarrow}_\Pi g_1 \cdots \overset{(t_i, v_i)}{\longrightarrow}_\Pi \cdots g_{m-1} \overset{(t_{m-1}, v_{m-1})}{\longrightarrow}_\Pi g_m,$$

  be a given minimum descendant chain from t to t'.
- **Conjecture**. There is an algorithm which constructs a descendant chain from f to t'. In particular,

$$\mathcal{D}(f) = \cup_{t \in \mathrm{Supp}(f) \cap T} \mathcal{D}(t).$$

- Corollary. $\mathcal{D}(t) \subseteq \mathcal{D}(f)$ for every $t \in \mathrm{Supp}(f) \cap T$.

Conjecture Relating Partial Order and Termination

- Define a binary relation $\prec$ on T by $t' \prec t$ if t' is a descendant of t. If Π is terminating, then $\prec$ is a partial order on T.

- **Conjecture**. Π is terminating if and only if there exists a well-order $\prec$ on T that is compatible with Π.

Why an abstract approach?

- Working in such generality requires obviously some justification; I hope the following are sufficient. Any time one introduces a new instantiation of standard bases, one has to define more or less the same concepts, to state more or less the same results and, what is worse, to provide more or less the same proofs; I hope that the general concepts, results and proofs provided by this paper will help new researchers to avoid this trivial but cumbersome burden.

Why an abstract approach?

- Working in such generality requires obviously some justification; I hope the following are sufficient. Any time one introduces a new instantiation of standard bases, one has to define more or less the same concepts, to state more or less the same results and, what is worse, to provide more or less the same proofs; I hope that the general concepts, results and proofs provided by this paper will help new researchers to avoid this trivial but cumbersome burden.

  — Teo Mora

  From: Seven variations on standard bases (1988)

- **Thank You.**

References

- Calogero G. Zarba, Lecture Notes in Decision Procedures, Ch. 1, Multi-sorted Logic, `http://web.archive.org/web/20070929131504/http://react.cs.uni-sb.de/~zarba/snow/ch01.pdf`

- Christoph Lüth, Compositional Term Rewriting: An Algebraic Proof of Toyama's Theorem (1996), in Rewriting Techniques and Applications, 7th International Conference, number 1103 in Lecture Notes in Computer Science.