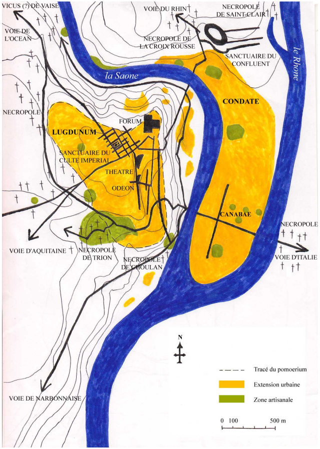
Musée des confluences

Philippe Malbos
Institut Camille Jordan
Université Claude Bernard Lyon 1



journée de l'équipe Algèbre, Géométrie, Logique
22 janvier 2015
Sainte Foy lès Lyon

Musée des confluences

Rewriting

- **Rewriting** arises in a variety of situations in Computer Science:
  - theory of programming languages: analysis, verification, optimisation,
  - Automated theorem proving.
- ... and in Algebra:
  - decision procedures for word problems in universal algebras,
  - in Computer Algebra: bases, syzygies, homology groups, Hilbert series, Koszulness,
  - Algebraic Coherence.

I. Equivalence Problem

Thue

Axel Thue, *Probleme über Veränderungen von Zeichenreihen nach gegebenen Regeln*, Christiana Videnskabs-Selskabs Skrifter, I. Math.-naturv. Klasse, 1914.

A. Thue (1863-1922)

- The notion of **rewriting system** was introduced by Thue when he considered systems of transformation rules for combinatorial objects such as strings, trees or graphs:

- He considered a system consisting of pairs of corresponding strings over a fixed alphabet:

$$\begin{array}{ccccc} A_1, & A_2, & A_3, & \dots & , A_n \\ B_1, & B_2, & B_3, & \dots & , B_n \end{array}$$

Thue Problem.

Given two arbitrary strings P and Q, can we get one from the other by replacing some substring A_i or B_i by its corresponding string?

Church-Rosser

A. Church (1903-1995)

Alonzo Church, J. Barkley Rosser, *Some properties of conversion*, Transactions of the AMS, 1936.

- Theory of reduction relations.

- S a set, $\longrightarrow$ a binary relation on S.
  - (x, y) in $\longrightarrow$ is denoted $x \longrightarrow y$ and we say x **reduces** to y.
  - Suppose $\longrightarrow$ recursive : given x, y in S, we can decide whether $x \longrightarrow y$.
  - Suppose that we can decide whether x in S is reducible, *i.e.*, $x \longrightarrow y$ for some y.

- Notations
  - $\longrightarrow^*$ the reflexive-transitive closure of $\longrightarrow$,
  - $\longleftrightarrow^*$ the reflexive-transitive-symmetric closure of $\longrightarrow$.

Equivalence Problem.

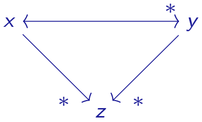
Decide $\longleftrightarrow^*$, i.e., to determine for x and y in S whether $x \longleftrightarrow^* y$.

Church-Rosser

- $\longrightarrow$ is **terminating**, or *Noetherian* if there is no infinite sequence

$$x_1 \longrightarrow x_2 \longrightarrow x_3 \longrightarrow \ldots \longrightarrow \ldots x_n \longrightarrow \ldots$$

- $\longrightarrow$ is **Church-Rosser** if $x \longleftrightarrow^* y$ implies $x \downarrow_* y$



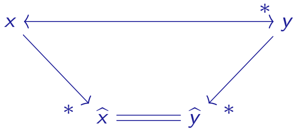
Church-Rosser

Theorem.

Let $\longrightarrow$ be terminating and Church-Rosser. Then the equivalence problem for $\longrightarrow$ is decidable.

Proof. Let x and y be in S. Let $\widehat{x}$ and $\widehat{y}$ be normal forms of x and y.

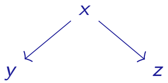
$$x \longleftrightarrow^* y \qquad \text{iff} \qquad \widehat{x} \longleftrightarrow^* \widehat{y} \qquad \text{iff} \qquad \widehat{x} \downarrow_* \widehat{y} \qquad \text{iff} \qquad \widehat{x} = \widehat{y}.$$



- The equivalence problem for $\longrightarrow$ could be decidable although
  - $\longrightarrow$ is not terminating

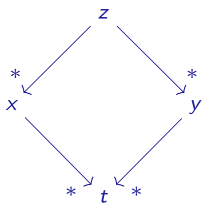
$$0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow \ldots \longrightarrow n \longrightarrow n+1 \longrightarrow n+2 \longrightarrow \ldots$$

  - $\longrightarrow$ is not Church-Rosser:

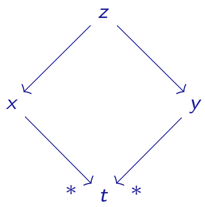


Newman

- $\longrightarrow$ is **confluent** if $x \uparrow^* y$ implies $x \downarrow_* y$



- $\longrightarrow$ is **locally confluent** if $x \uparrow y$ implies $x \downarrow_* y$



Newman

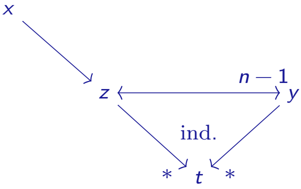
M. H. A. Newman
(1897-1984)

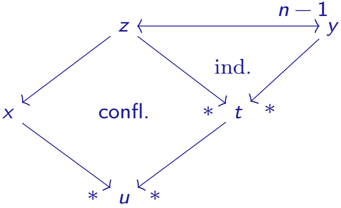
Maxwell H. A. Newman. *On theories with a combinatorial definition of "equivalence"*, Annals of Math., 1942.

Theorem. (Newman, 1942)
$\longrightarrow$ is Church-Rosser if and only if $\longrightarrow$ is confluent.

Proof.
Church-Rosser implies confluent. Suppose $\longrightarrow$ confluent and proceed by induction.

Suppose $x \longleftrightarrow^n y$. Case $n = 0$ is immediate. Suppose $n > 0$.





Newman

Theorem. (Newman, 1942) (**Newman diamond Lemma**)

Let $\longrightarrow$ terminating. Then $\longrightarrow$ is confluent if and only if $\longrightarrow$ is locally confluent.

▶ **Principle of Noetherian induction**. Suppose $\longrightarrow$ terminating. Let $\mathbf{P}$ be a predicate on S.

If for all x in S

$$\left[\text{ for all } y \text{ in } S,\ x \longrightarrow y \text{ implies } \mathbf{P}(y) \right] \text{ implies } \mathbf{P}(x)$$

then

$$\text{for all } x \text{ in } S,\ \mathbf{P}(x).$$

See Huet, 1980, Cohn, 1974 for a correctness proof.

Newman

Theorem. (Newman, 1942) (**Newman diamond Lemma**)

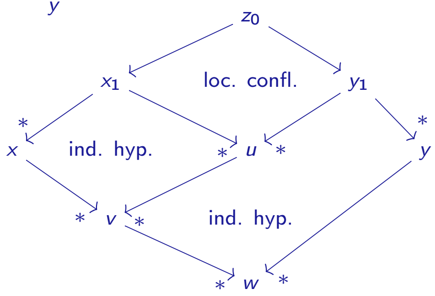
Let $\longrightarrow$ terminating. Then $\longrightarrow$ is confluent if and only if $\longrightarrow$ is locally confluent.

Proof. (see Huet, 1980)

- ▷ Confluence implies local confluence.
- ▷ Suppose $\longrightarrow$ locally confluent and proceed by Noetherian induction.
- ▷ Induction hypothesis:

  for all z with $z_0 \longrightarrow z$ and for all $x' \overset{*}{\longleftarrow} z \overset{*}{\longrightarrow} y'$ we have $x' \overset{*}{\longrightarrow} t \overset{*}{\longleftarrow} y'$

- ▷ Suppose $x \overset{*}{\longleftarrow} z_0 \overset{*}{\longrightarrow} y$ Cases $x = z_0$ and $y = z_0$ are obvious.

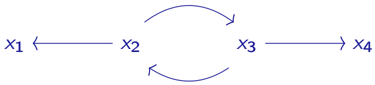


Newman

Theorem. (Newman, 1942) (**Newman diamond Lemma**)

Let $\longrightarrow$ terminating. Then $\longrightarrow$ is confluent if and only if $\longrightarrow$ is locally confluent.

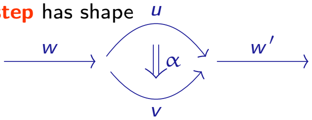
- The requirement of Noetherianity is necessary:



II. Word Problem and Homology of Monoids

Knuth-Bendix

- **String rewriting system** defined by a set X and a set of **rules** R on X^*.
  - ▷ A **rewriting step** has shape

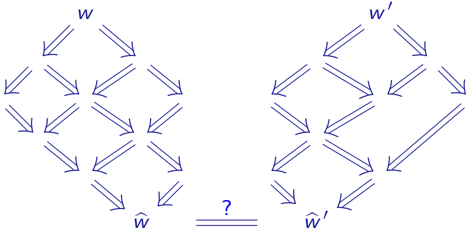


$u \overset{\alpha}{\Longrightarrow} v$ in R.

- **Word Problem** for a monoid $\mathbf{M}$ presented by $\langle X \mid R \rangle$:
  - ▷ two word w and w' in X^*,
  - ▷ does $w = w'$ hold in $\mathbf{M}$?

- **Normal form algorithm**.

  ▷ If $\mathbf{M}$ has a finite **convergent** (confluent and terminating) presentation then its Word Problem is decidable:



Knuth-Bendix

Maurice Nivat, *Congruences parfaites et quasi-parfaites*, Séminaire Dubreuil, 1971-1972.

▶ One can decide whether a finite string rewriting system is convergent by checking local confluence.

M. Nivat (1937-)

Theorem.

Let $\langle X \mid R \rangle$ be a finite terminating string rewriting system. Then, whether or not R is locally confluent, is decidable. Hence, it is decidable whether or not R is confluent.

Proof.

The proof involves the notion of **critical branching** which corresponds to a minimal overlapping application of two rules on the same string: situations:

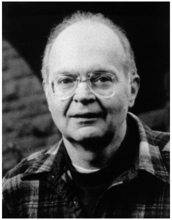
▷ If R is finite, there are only finitely many critical branchings.

▷ It thus can be tested whether every such branching is confluent.

▷ $\langle X \mid R \rangle$ is locally confluent if and only if every critical branching is confluent.

Knuth-Bendix

Donald Knuth, Peter Bendix, *Simple Word Problems in Universal Algebras*, 1970.



D. Knuth (1938-)

- Completion procedure.

- Knuth-Bendix completion procedure, 1970.
  - Input : a rewriting system $\langle X \mid R \rangle$ and a Noetherian order $<$ on X^*
  - by adding new rules, compute a set of rule $\widetilde{R}$ suhc that

    i) for all $u \Rightarrow v$ in $\widetilde{R}$, we have $v < u$,

    ii) $\widetilde{R}$ is confluent,

    iii) $\widetilde{R}$ and R are Tietze equivalents.

- Procedure terminates if and only if there is a finite set R such that **i)**, **ii)**, **iii)** hold.
  - else it may run for ever adding **infinitely** many new rules such that **i)**, **ii)**, **iii)** hold.
  - it may also terminate with **failure** if one of the input identities cannot be ordered by $<$.

Jantzen

Question. (Jantzen, 1982)

Does every finitely presented monoid with a decidable word problem admit a finite convergent presentation?

Example. (Kapur-Narendran, 1985)

$$\mathbf{B}_3^+ = \langle\, s, t \mid sts = tst \,\rangle$$

- ▷ The monoid $\mathbf{B}_3^+$ is decidable.
- ▷ It admits no finite convergent presentation on the two generator s and t

... but with 3 generators (Bauer-Otto, 1984).

- ▷ by adjunction of a new generator a standing for the product st :

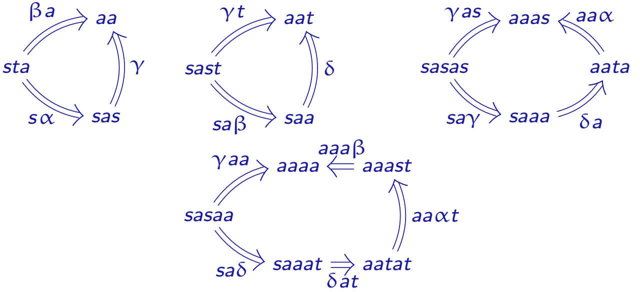
$$\Sigma^{BO} = \langle\, s, t, a \;\big|\; ta \overset{\alpha}{\Longrightarrow} as,\; st \overset{\beta}{\Longrightarrow} a \,\rangle.$$

Jantzen

Example. Knuth-Bendix completion of the rewriting system

$$\Sigma^{\mathrm{BO}} = \langle\, s, t, a \mid ta \overset{\alpha}{\Longrightarrow} as,\; st \overset{\beta}{\Longrightarrow} a \,\rangle$$

$$\mathcal{KB}(\Sigma^{\mathrm{BO}}) = \langle\, s, t, a \mid ta \overset{\alpha}{\Longrightarrow} as,\; st \overset{\beta}{\Longrightarrow} a,\; sas \overset{\gamma}{\Longrightarrow} aa,\; saa \overset{\delta}{\Longrightarrow} aat \,\rangle$$



Conséquence.

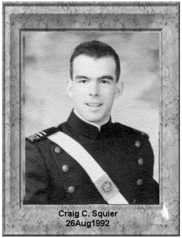
The word problem for $\mathbf{B}_3^+$ is solvable by the normal form algorithm

Question.

Which condition a monoid need to satisfy to admit a presentation by a finite convergent rewriting system?

Squier

Craig C. Squier, *World problems and a homological finiteness condition for monoids*, J. Pure Appl. Algebra, 1987.



C. C. Squier
(1946-1992)

Theorem. (Squier, 1987)

If a monoid $\mathbf{M}$ admits a finite convergent presentation, then it is of homological type left-FP_3.

In particular, the group $\mathrm{H}_3(\mathbf{M}, \mathbb{Z})$ is finitely generated.

Examples. (Squier, 1987, Stallings, 1963, Abels, 1979)

There are finitely presented monoids with a decidable word problem which do not have homological type left-FP_3.

Consequence.

Rewriting is not universal to decide Word Problem in finitely presented monoids.

Theorem. (Anick, 1987, Kobayashi, 1991, Groves, 1990, Brown, 1992)

If a monoid $\mathbf{M}$ admits a finite convergent presentation, then it is of homological type left-FP_∞.

III. Linear Rewriting

Buchberger

Bruno Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal*, Ph.D. thesis, Univ. of Innsbruck, 1965.

B. Buchberger (1942-)

Original Problem.

- Given $\mathbf{F}$, a finite set of polynomials of $\mathbb{K}[\mathbf{x_1}, \ldots, \mathbf{x_n}]$.
- Find a linearly basis for the algebra $\mathbb{K}[\mathbf{x_1}, \ldots, \mathbf{x_n}]/\langle \mathbf{F} \rangle$.

- Fix an admissible ordering. Given $\mathbf{f}, \mathbf{g}, \mathbf{h}$ polynomials in $\mathbb{K}[\mathbf{x_1}, \ldots, \mathbf{x_n}]$.
  - $\mathbf{f}$ **reduce** into $\mathbf{h}$ modulo $\mathbf{g}$:

$$\mathbf{f} \longrightarrow_{\mathbf{g}} \mathbf{h},$$

if $\mathrm{lm}(\mathbf{g})$ divide a term $\mathbf{X}$ in $\mathbf{f}$ and

$$\mathbf{h} = \mathbf{f} - \frac{\mathbf{X}}{\mathrm{lt}(\mathbf{g})}\mathbf{g}. \qquad \mathrm{lt}(\mathbf{f}) \longrightarrow_{\mathbf{f}} \mathrm{lt}(\mathbf{f}) - \mathbf{f}.$$

- $\mathbf{f}$ *reduce* into $\mathbf{h}$ modulo $\mathbf{F}$, $\mathbf{f} \longrightarrow_{\mathbf{F}} \mathbf{h}$, if

$$\mathbf{f} \xrightarrow{f_{i_1}} \mathbf{h_1} \xrightarrow{f_{i_2}} \mathbf{h_2} \xrightarrow{f_{i_3}} \ldots \mathbf{h_{i_{k-1}}} \xrightarrow{f_{i_k}} \mathbf{h}, \qquad \text{with } \mathbf{f_{i_j}} \in \mathbf{F}.$$

- If $\mathbf{f} \longrightarrow_{\mathbf{F}} \mathbf{r}$, where $\mathbf{r}$ is a normal form, then $\mathbf{r}$ is the remainder of the division of $\mathbf{f}$ with respect to divisors in $\mathbf{F}$.

Buchberger

Let $G = \{g_1, \ldots, g_t\}$ be a subset of polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ and let $I = \langle\, G \,\rangle$.

- The subset G is a **Gröbner basis** for I if $\longrightarrow_G$ is Church-Rosser.

Theorem.

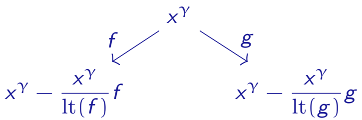
The following are equivalent

i) G is a Gröbner basis for I,
ii) $\longrightarrow_G$ is confluent,
iii) $\langle\, \mathrm{lt}(I) \,\rangle = \langle\, \mathrm{lt}(G) \,\rangle$,
iv) $f \longrightarrow_G^* 0$ for every f in I,
v) for all $i \neq j$, $S(g_i, g_j) \longrightarrow_G^* 0$.

- ***S*-polynomial** of f and g:

$$S(f, g) = \frac{x^\gamma}{\mathrm{lt}(f)} f - \frac{x^\gamma}{\mathrm{lt}(g)} g, \qquad x^\gamma = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)).$$

  - S-polynomials correspond to critical branchings:



Buchberger

- **Buchberger algorithm** for computing a Gröbner basis.

INPUT: $F = \{f_1, \dots, f_s\}$ a basis of I, with $f_i \neq 0$.

OUTPUT: a Gröbner basis G of I with $F \subset G$.

Initialisation:

$G := F$

$\mathcal{G} := \{\, \{f_i, f_j\} \mid f_i \neq f_j \in G\}$

while $\mathcal{G} \neq \emptyset$ **do**

choose $\{f, g\} \in \mathcal{G}$

$\mathcal{G} := \mathcal{G} - \{\{f, g\}\}$

$S(f, g) \xrightarrow{G} r$, where r is a normal form

if $r \neq 0$ **then**

$\mathcal{G} := \mathcal{G} \cup \big\{\{f, r\} \mid \text{for every } f \in G\big\}$

$G := G \cup \{r\}$

Gröbner-Shirshov

- **Gröbner-Shirshov bases**:
  - A. I. Shirshov, *Some algorithmic problem for Lie algebras*, Sibirsk Mat. Zh., 1962.
  - How to find a linear basis of any Lie algebra presented by generators and relations ?
  - A critical branching/completion algorithm based on **composition** (S-polynomial).

- For associative algebras : Bokut, 1976, Bergman, 1978, Mora, 1986.

- For operads, Dotsenko-Khoroshkin, 2010.

- For linear categories without monomial order, Guiraud-Hoffbeck-M., 2014.

- Heisuke Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero*, 1964.

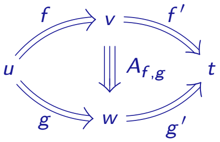
- Maurice Janet, *Sur les systèmes d'équations aux dérivées partielles*, 1920.

III. Rewriting and Algebraic Coherence

Algebraic Coherence

Theorem. (Squier, 1994)

Let $\langle X \mid R \rangle$ be a convergent rewriting system. Then the set of confluences

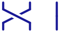
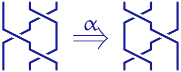


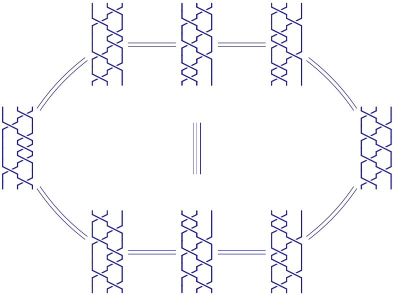
indexed by critical branching (f, g), forms a homotopy basis of derivation graph of $\langle X \mid R \rangle$.

Algebraic Coherence

Example.

$$\mathrm{Art}_3(\mathbf{S}_3) = \langle\ s, t \mid tst \overset{\alpha}{\Longrightarrow} sts \mid \emptyset\ \rangle$$

$s =$  $t =$  



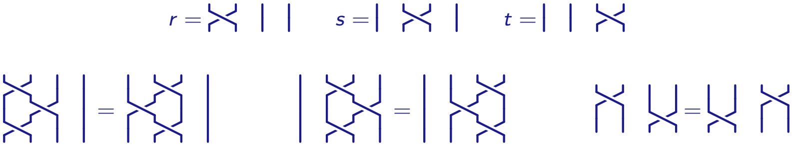
Proposition.

For presentation $\mathrm{Art}_2(\mathbf{S}_3)$ of $\mathbf{B}_3^+$ two proofs of the same equality are equals.

Algebraic Coherence

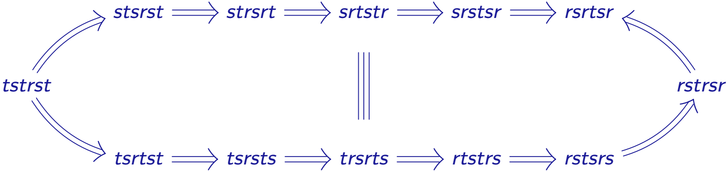
Exemple.

$$\mathrm{Art}_2(\mathbf{S}_4) = \langle\, r, s, t \mid rsr = srs,\ sts = tst,\ rt = tr \,\rangle$$



Proposition. (Deligne, 1997)

For presentation $\mathrm{Art}_2(\mathbf{S}_4)$ of $\mathbf{B}_4^+$ two proof of the same equality are equals modulo **Zamolodchikov relation**



Algebraic Coherence

Theorem. [Gaussent-Guiraud-M., 2013]

For every Coxeter group $\mathbf{W}$ with a totally ordered set S of generators, the Artin monoid $\mathbf{B}^+(\mathbf{W})$ admits the coherent presentation $\mathrm{Art}_3(\mathbf{W})$ made of

▷ Artin's presentation

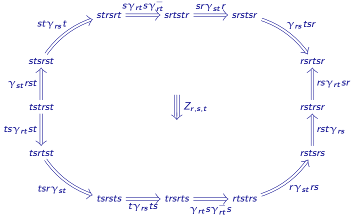
$$\mathrm{Art}_2(\mathbf{W}) = \langle\ S \mid \langle ts \rangle^{m_{st}} \ = \ \langle st \rangle^{m_{st}}\ \rangle$$

▷ one 3-cell $Z_{r,s,t}$ for every elements $t > s > r$ of S such that the subgroup $\mathbf{W}_{\{r,s,t\}}$ is finite.

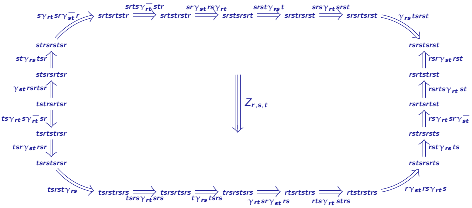
▶ In this way, we obtained a constructive proof of the Tits results, 1981.

Algebraic Coherence

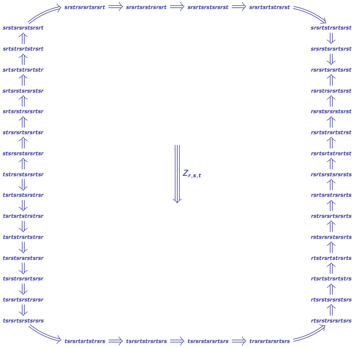
Type A_3



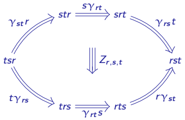
Type B_3



Type H_3



Type $A_1 \times A_1 \times A_1$



Type $I_2(p) \times A_1$, $p \geqslant 3$,