Diagram Rewriting

Yves Lafont
CNRS - Institut de Mathématiques de Luminy
Université de la Méditerranée (Aix-Marseille 2)

Thematic school: Operads
CIRM - Marseille
April 2009

Word problem

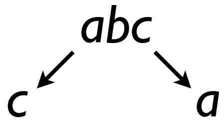
In a noncommutative monoid:

- Knowing that $ab = 1$,
  can we deduce that $ba = 1$? **NO**
- Knowing that $ab = 1 = bc$,
  can we deduce that $ba = 1$? **YES**

$$ba = babc = bc = 1$$

Word rewriting

- *ab* → 1: *convergent* rewrite system;
- *ab* → 1, *bc* → 1: *nonconvergent* rewrite system.

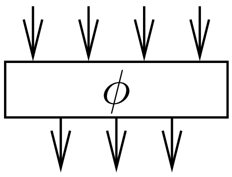


But in general, the word problem is *undecidable*.

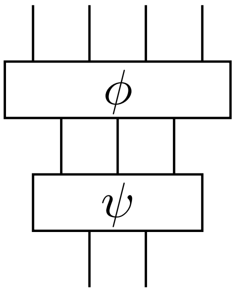
(even for groups)

Diagrams

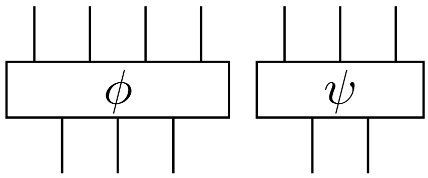
Inputs/outputs



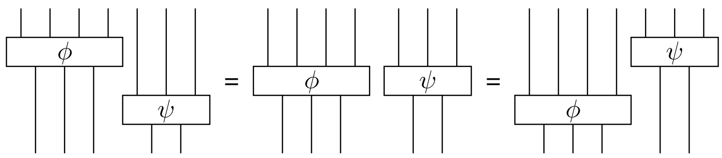
Sequential composition



Parallel composition



Interchange



Terminology

- *basic case*: + (disjoint union)

$$f : p \to q \qquad (p = \{1, \ldots, p\} = 1 + \cdots + 1)$$

- *classical case*: x (cartesian product)

$$f : \mathbf{B}^p \to \mathbf{B}^q \qquad (\mathbf{B} = \{0,1\} = 1 + 1,\ \mathbf{B}^p = \mathbf{B} \times \cdots \times \mathbf{B})$$

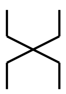
- *linear case*: $\bigoplus$ (direct sum)

$$f : \mathbb{Z}_2^p \to \mathbb{Z}_2^q \qquad (\mathbb{Z}_2 = \{0,1\},\ \mathbb{Z}_2^p = \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2)$$

- *quantum case*: $\bigotimes$ (tensor product)

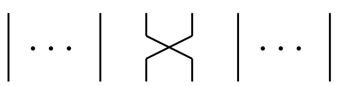
$$f : \mathbb{B}^{\otimes p} \to \mathbb{B}^{\otimes q} \qquad (\mathbb{B} = \mathbb{C}^2 = \mathbb{C} \oplus \mathbb{C},\ \mathbb{B}^{\otimes p} = \mathbb{B} \otimes \cdots \otimes \mathbb{B})$$

First example: Finite permutations

Generator 

Relations 

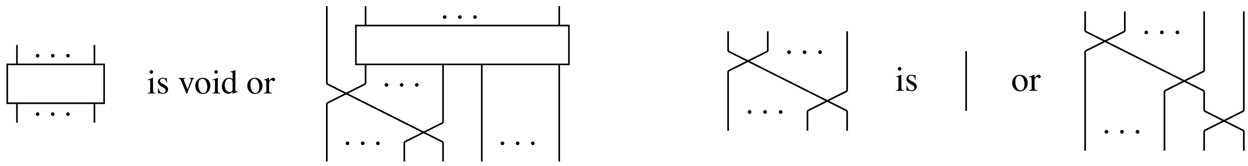
- Any finite permutation is a product of transpositions.



- Two diagrams define the same permutation if and only if they are equivalent modulo the above relations.

Canonical forms

Grammar for *canonical forms*:

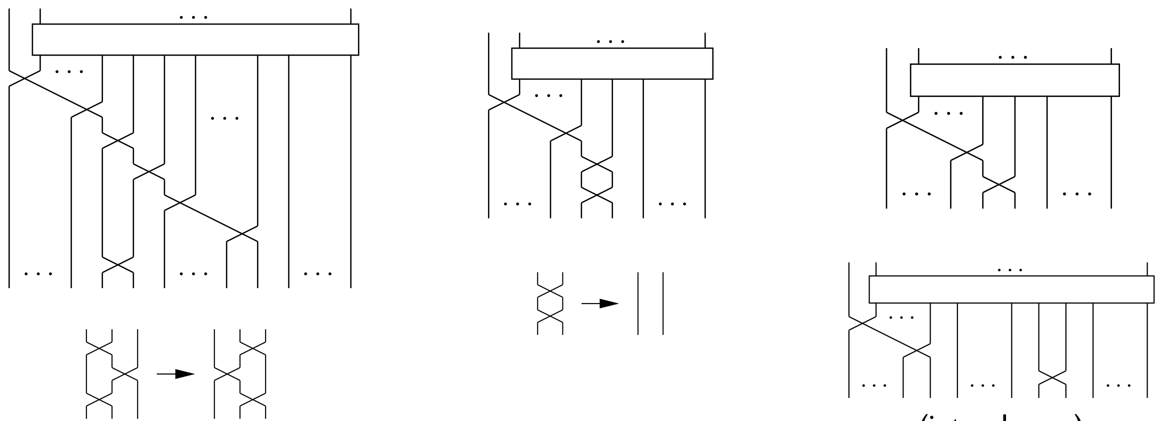


- Any permutation corresponds to a unique canonical form.
- Any diagram reduces to a canonical form by the following two *rewrite rules*:

Reduction to the canonical form

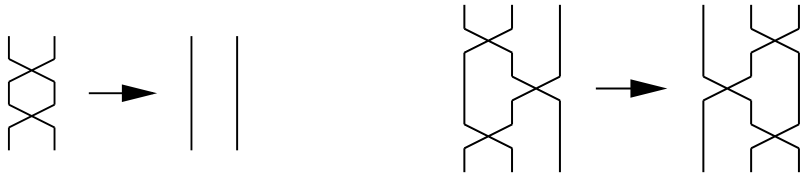
By double induction:

- on the *width* (number of wires);
- on the *size* (total number of gates).



(interchange)

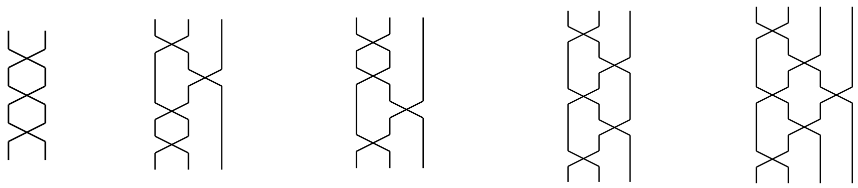
Rewriting



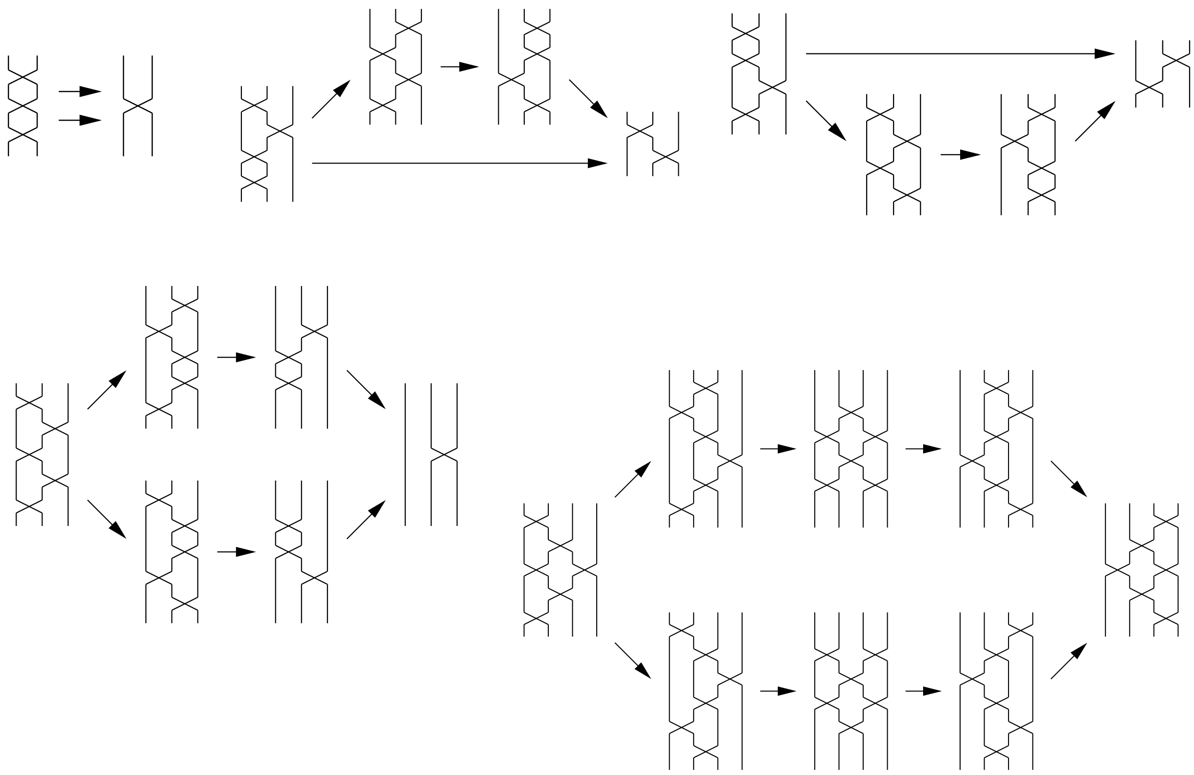
This rewrite system is *convergent*:

- *termination* (existence of a canonical form);
- *confluence* (uniqueness of the canonical form).

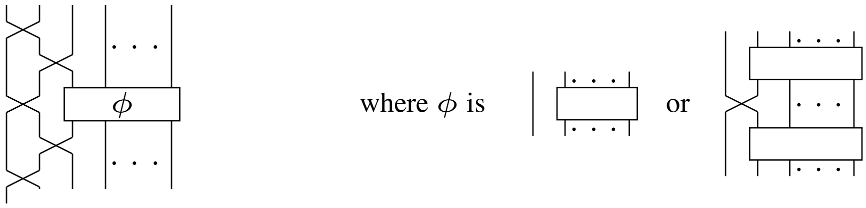
Conflicts (*critical peaks*)



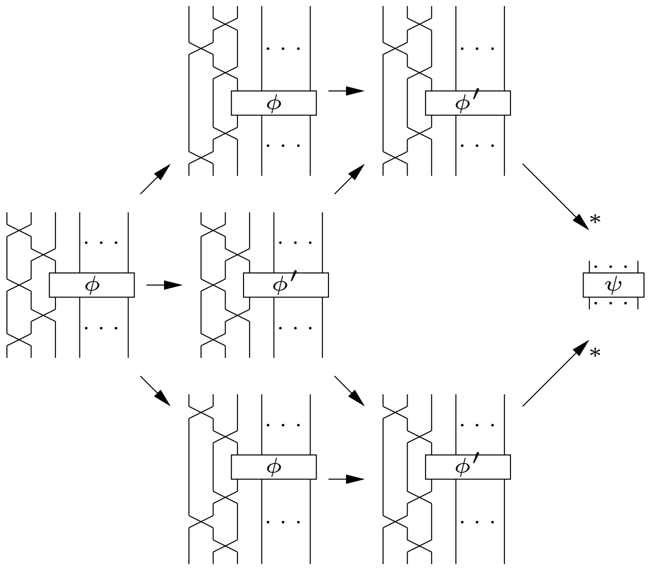
Confluence of critical peaks



Confluence of global conflicts

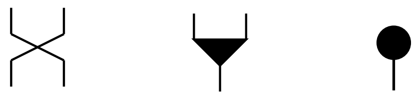


By induction:

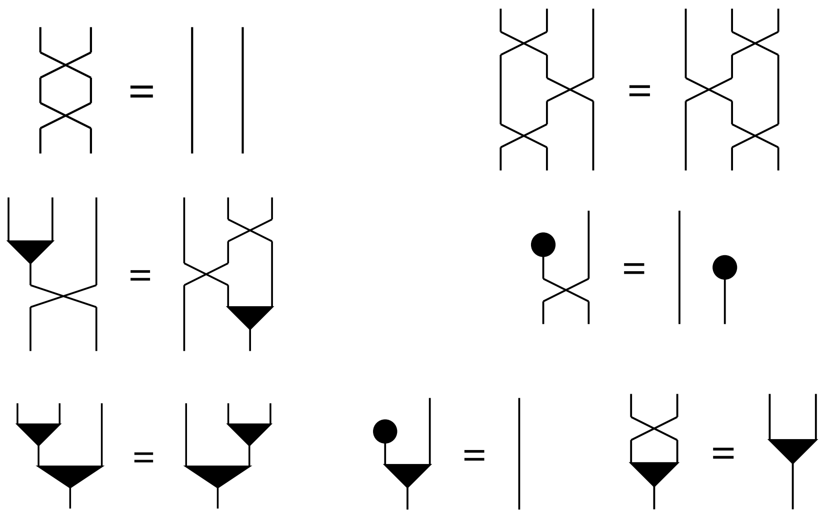


Second example: Finite maps

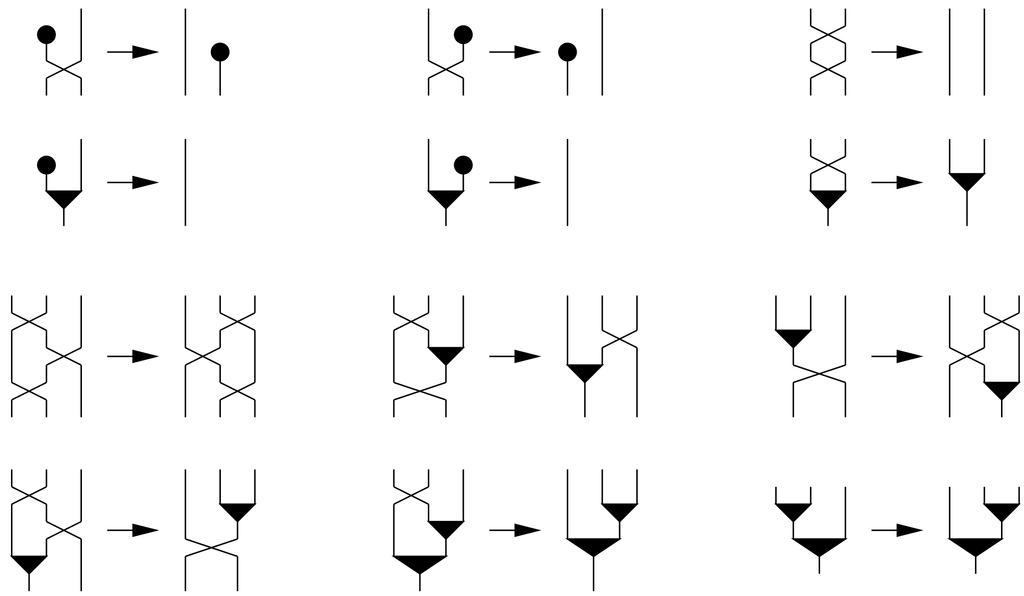
Generators



Relations

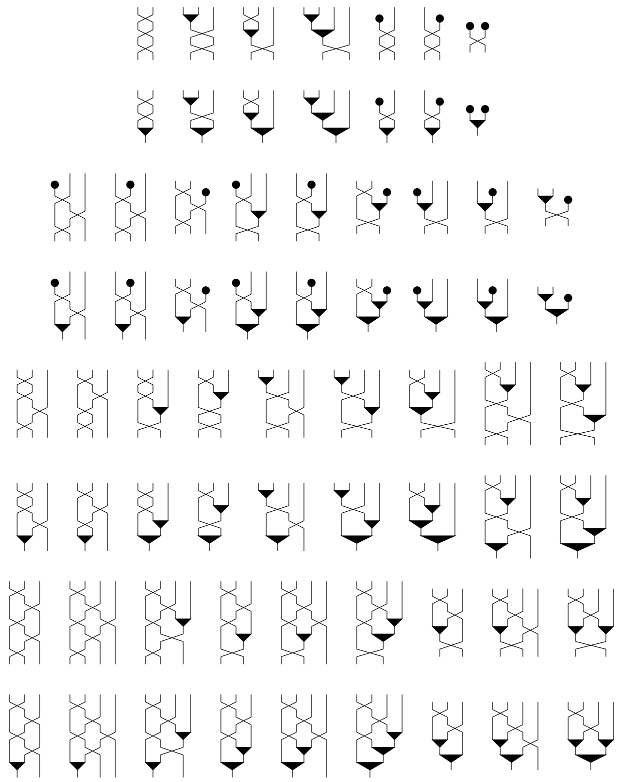


Rewrite rules



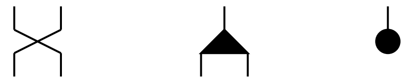
This rewrite system is convergent.

68 critical peaks

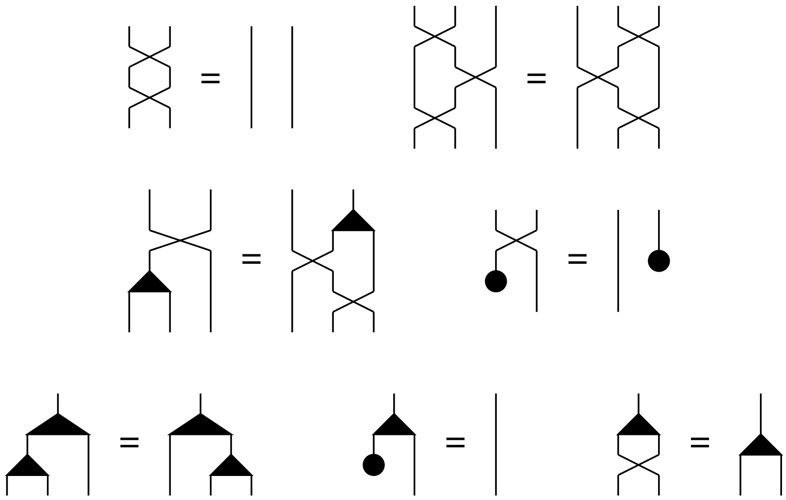


Third example: dual of finite maps

Generators

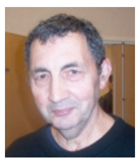


Relations



Terms versus diagrams

- Any finite equational theory (with terms) yields a finite presentation (with diagrams) [Burroni 1991].

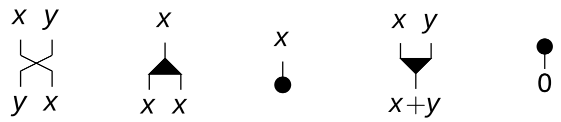


- Any finite convergent left linear rewrite system (with terms) yields a finite convergent rewrite system (with diagrams) [Lafont 1995].

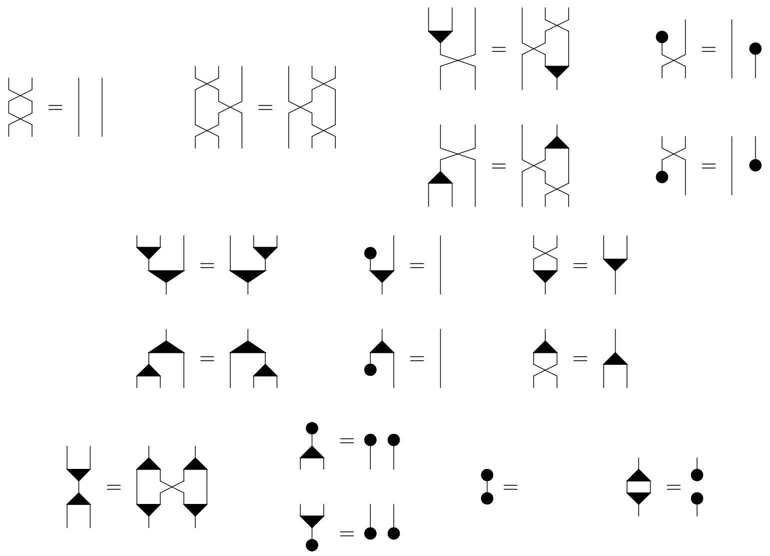
The non linear case is more difficult (critical peaks).

Fourth example: linear boolean maps

Generators



Relations

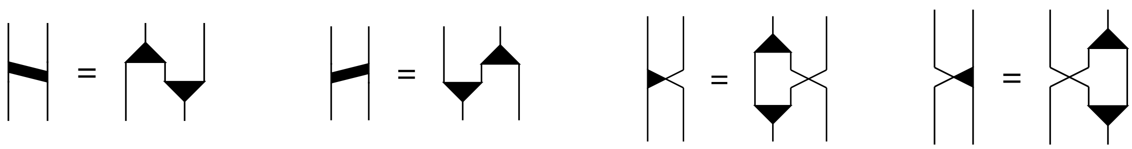


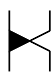
Reversible gates

Matrices

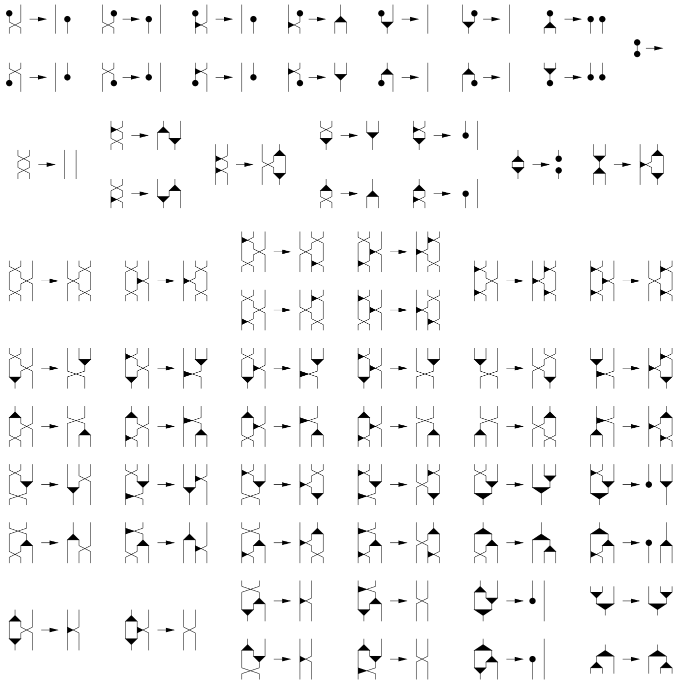
$$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} \quad \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}$$

Decompositions



We shall only use the third gate: 

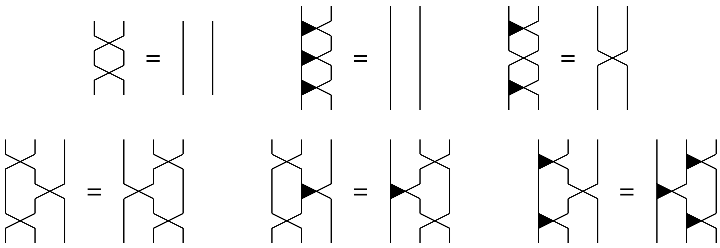
Convergent rewrite system



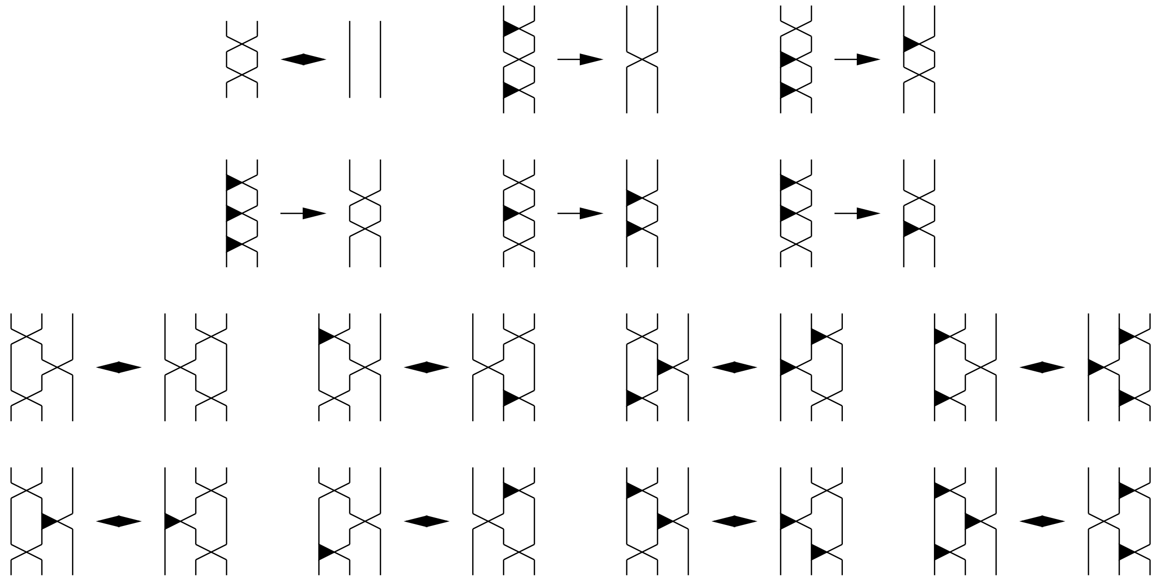
Fifth example: linear boolean permutations

Generators

Relations



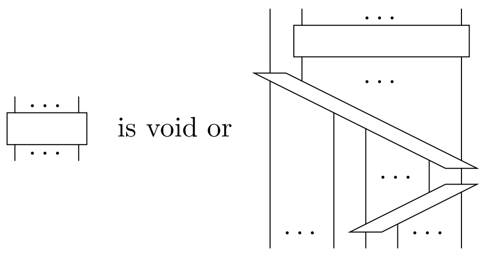
Rewrite rules



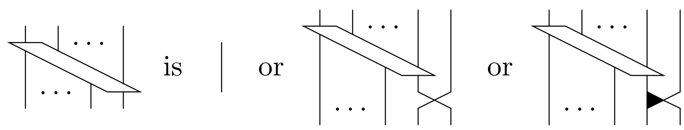
(no termination)

Canonical forms

Grammar for canonical forms:

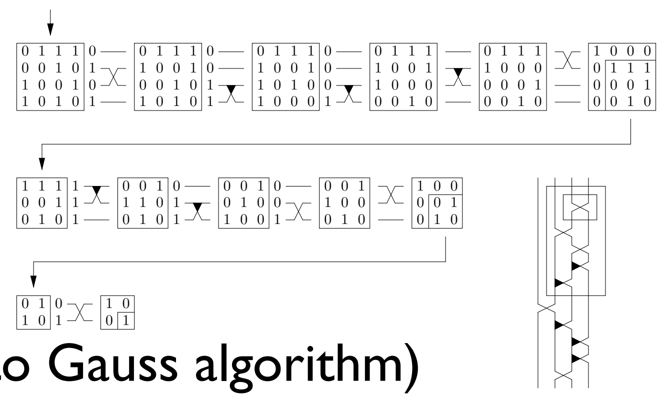


Stairs



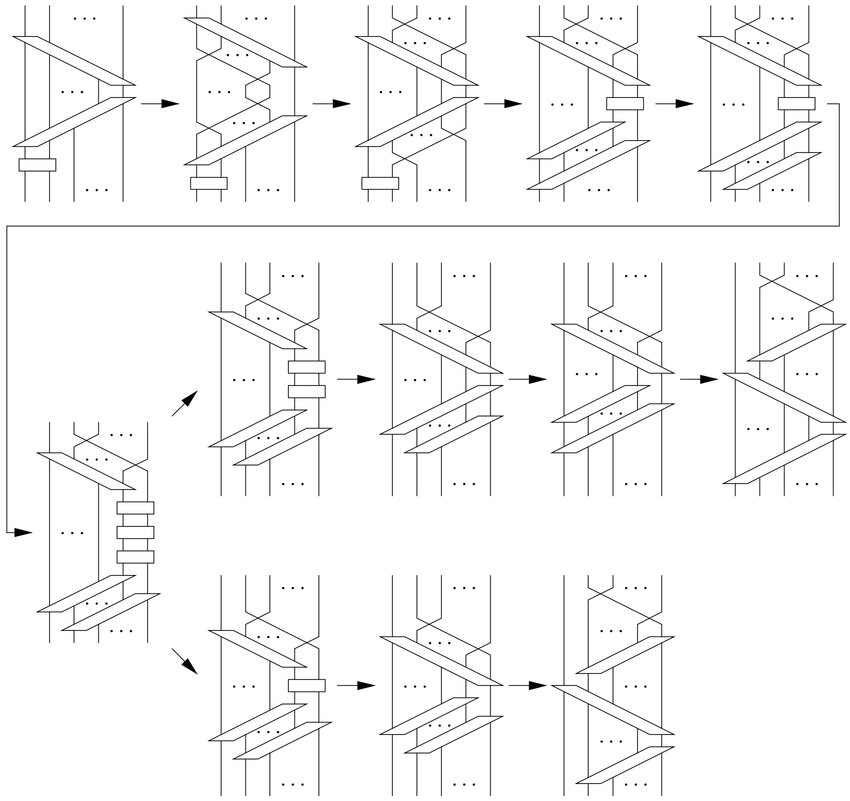
Idem for *antistairs*

Computing the canonical form:



(similar to Gauss algorithm)

Crucial lemma



References

- Albert Burroni, *Higher dimensional word problems* (TCS 1993)
- Yves Lafont, *Towards an algebraic theory of Boolean circuits* (JPAA 2003)
- Yves Guiraud, *Termination Orders for 3-Dimensional Rewriting* (JPAA 2006)
- Yves Lafont, *Algebra and geometry of rewriting* (ACS 2007)
- Yves Lafont & Pierre Rannou, *Diagram rewriting for orthogonal matrices* (RTA 2008)
- Yves Lafont, *Réécriture et problème du mot* (Gazette de la SMF 2009)