Homotopy and Homology of Rewriting

Yves Lafont
Institut de Mathématiques de Marseille

International School on Rewriting, Paris, 3-4 July

Part 1 : Word rewriting

Presentations of monoids

generators	relations	monoid
a	$a^2 = 1$	$\mathbb{Z}_2$ (*integers modulo 2*)
a	$a^2 = a$	$\mathbb{N}_2$ (free *idempotent*)
a, a’	aa’ = 1, a’a = 1	$\mathbf{F}_1 = \mathbb{Z}$ (free *group*)
a, b	ab = ba	$\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$
a, a’, b, b’	aa’ = 1, a’a = 1, bb’ = 1, b’b = 1	$\mathbf{F}_2 = \mathbb{Z} * \mathbb{Z}$ (free *group*)
a, b	$a^2 = 1$, $b^2 = 1$, aba = bab	$\mathbf{S}_3$ (*symmetric group*)
a, b	aba = bab	$\mathbf{B}_3^+$ (*positive braids*)

Exercise : Give presentations for $\mathbb{Z}^2$ and for $\mathbf{B}_3$.

Standard presentation

Remark : Any (finite) monoid has a (finite) presentation.

Let M be any monoid.

	generators	**relations**
standard presentation	a_x ($x \in M$)	$a_x a_y = a_{xy}$, $a_1 = 1$
reduced standard presentation	a_x ($x \in M$, $x \neq 1$)	$a_x a_y = a_{xy}$ ($xy \neq 1$), $a_x a_y = 1$ ($xy = 1$)

Exercise : Give the standard presentation of $\mathbb{Z}_2$ and the reduced standard one.

Reductions and derivations

Definition : A *presentation* of a monoid M is given by a set Σ of *symbols* together with a set $R \subset \Sigma^* \times \Sigma^*$ of *rules* such that

$$M \simeq \Sigma^*/\leftrightarrow^*_R.$$

notion	**notation**	**definition**
word	$x \in \Sigma^*$	finite sequence of symbols $x = a_1 \cdots a_n$
elementary reduction	$u\rho v : uxv \rightarrow_R uyv$	$\rho : x \rightarrow y$ is a rule u, v are words
reduction	$x \rightarrow^*_R y$	finite chain $x \rightarrow_R \cdots \rightarrow_R y$
elementary derivation	$x \leftrightarrow_R y$	$x \rightarrow_R y$ or $y \rightarrow_R x$
derivation	$x \leftrightarrow^*_R y$	finite chain $x \leftrightarrow_R \cdots \leftrightarrow_R y$

Termination

Definition : A *termination ordering* is a well ordering on Σ^* which is compatible with multiplication.

Theorem : For a presentation (Σ,R), the following three conditions are equivalent:

There is no infinite reduction:

$x_0 \to_R x_1 \to_R \cdots \to_R x_n \to_R x_{n+1} \to_R \cdots$

There is some termination ordering on Σ^* such that $x > y$ for each rule $\rho : x \to y$ in R.

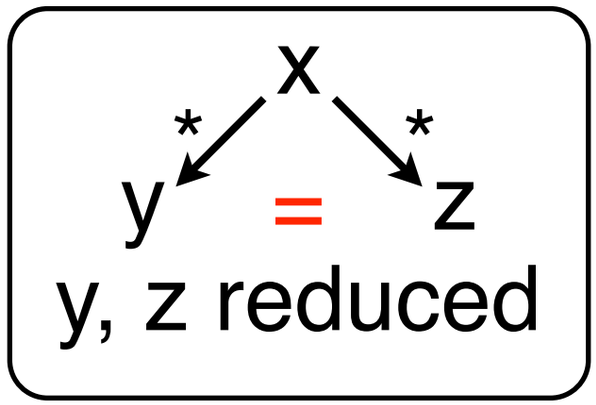
(Σ,R) satisfies a principle of *noetherian induction*:

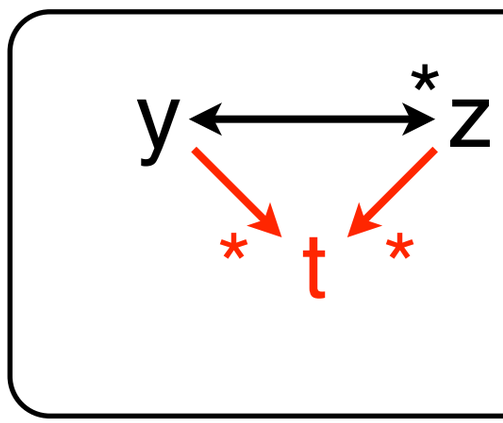
$(\forall x\in\Sigma^*(\forall y\in\Sigma^* x \to_R y \Rightarrow P(y)) \Rightarrow P(x)) \Rightarrow \forall x\in\Sigma^* P(x)$

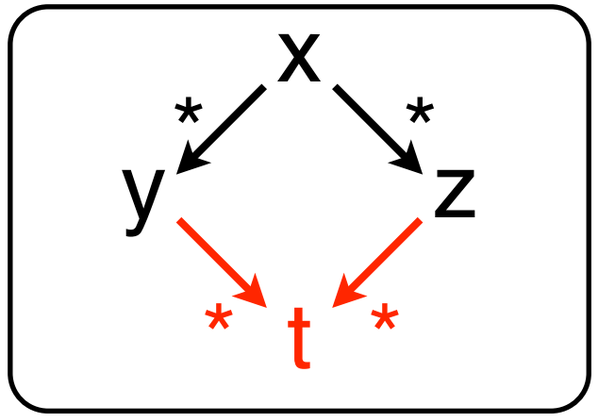
Then we say that the presentation (Σ,R) is *noetherian*.

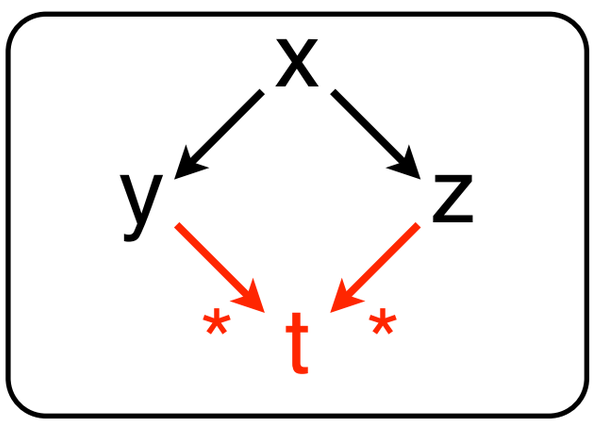
Confluence

Theorem : For a noetherian presentation, the following four conditions (*uniqueness of the reduced form*, *Church-Rosser property*, *global* and *local confluence*) are equivalent:



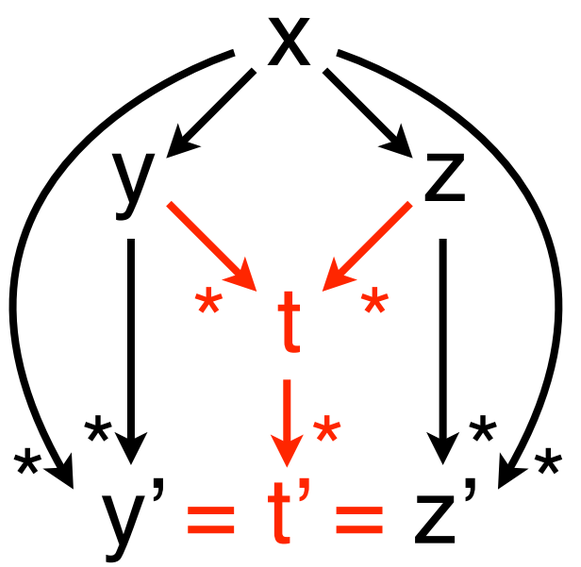






Proof : 1 ⇒ 2 ⇒ 3 ⇒ 4 (obvious)

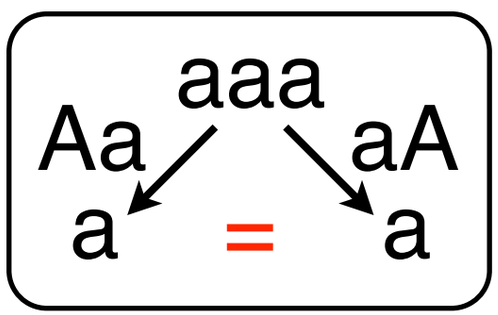
4 ⇒ 1 (by noetherian induction)

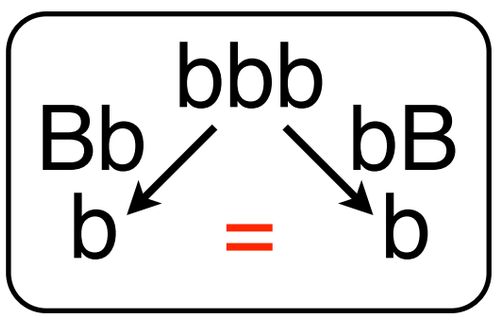


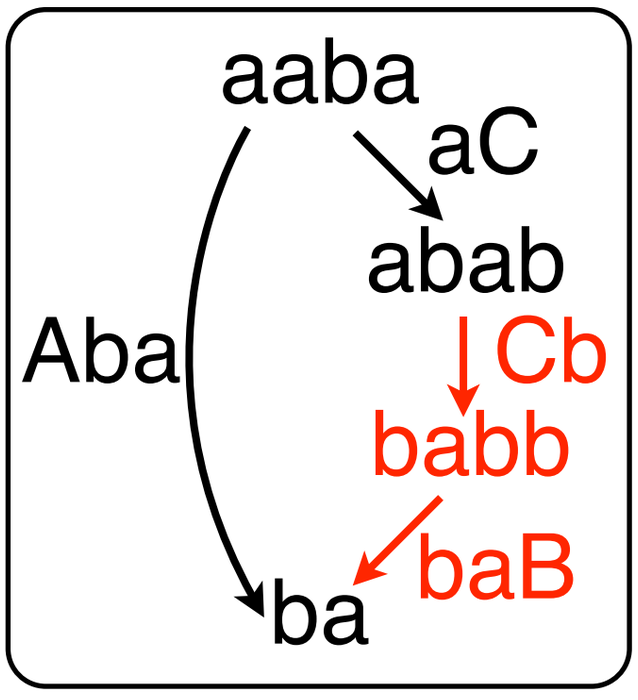
Confluence of critical peaks

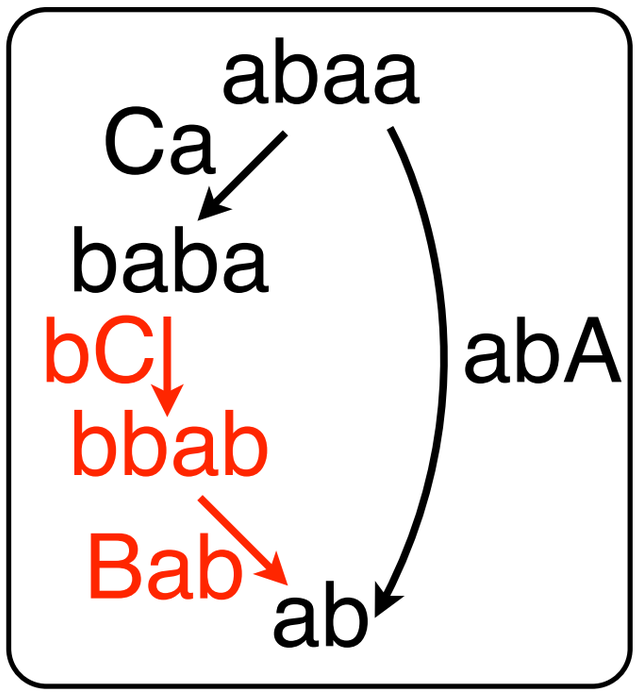
Theorem : To check local confluence,
il suffices to test confluence of *critical peaks*.

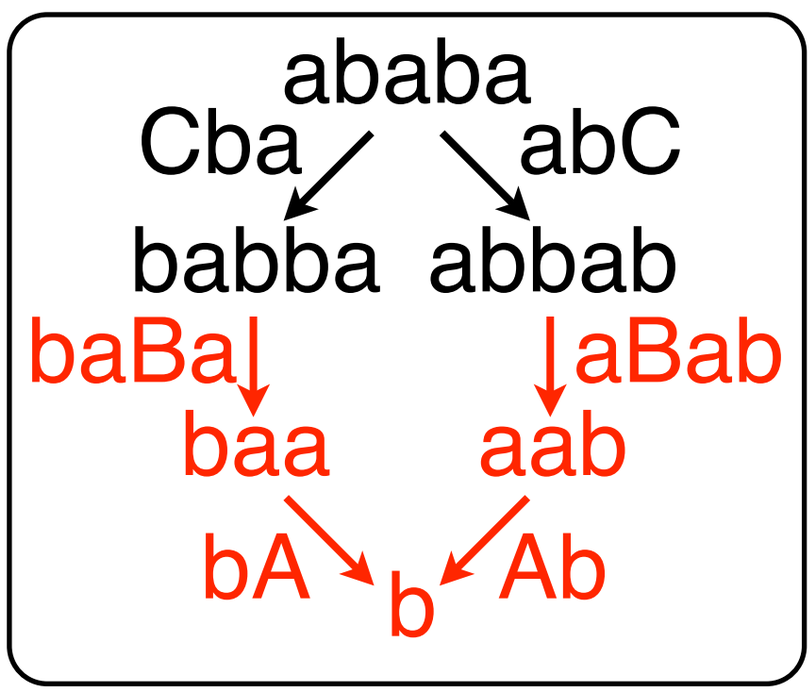
Example : $aa \xrightarrow{A} 1$, $bb \xrightarrow{B} 1$, $aba \xrightarrow{C} bab$











Exercise : The *standard presentation* is confluent.

Convergent presentations

notion	definition
convergent presentation	termination + confluence
reduced presentation	reduced generators + *minimal* left members + reduced right members
orthogonal presentation	no critical peak

Remark : Any (finite) convergent presentation is equivalent to a (finite) reduced convergent presentation.

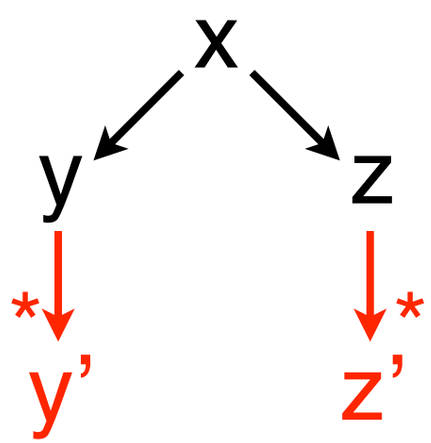
Exercise : Any orthogonal presentation is confluent.

Exercise : A (non trivial) group has no orthogonal convergent presentation.

Knuth-Bendix completion

Remark : There is some total termination ordering on Σ^*.

Algorithm : Reduce both sides of each critical peak :



- if y' = z', then it is already confluent
- if y' > z', add the rule y' → z'
- si y' < z', add the rule z' → y'
- eliminate superfluous rules

Exercise : Apply this algorithm to the following rules :
aa' → 1, a'a → 1, bb' → 1, b'b → 1, ba → ab

Exercise : Apply this algorithm to the rule bab → aba.
Idem by adding a generator c with the rule ab → c.

Word problem

Let (Σ,R) be a *finite* presentation of monoid.

problem	**data**	**question**
equivalence	$x, y \in \Sigma^*$	$x \leftrightarrow^*_R y$?
unit (by derivation)	$x \in \Sigma^*$	$x \leftrightarrow^*_R 1$?
unit (by reduction)	$x \in \Sigma^*$	$x \rightarrow^*_R 1$?

The second one is the *word problem*.

Remark : For a finite convergent presentation, all those problems are decidable.

Exercise : There is a finite orthogonal presentation for which those problems are undecidable. [Code the *halting problem*.]

Theorem (Novikov-Boone) : There is a finite presentation of group for which the word problem is undecidable.

Part 2 : Homology of rewriting

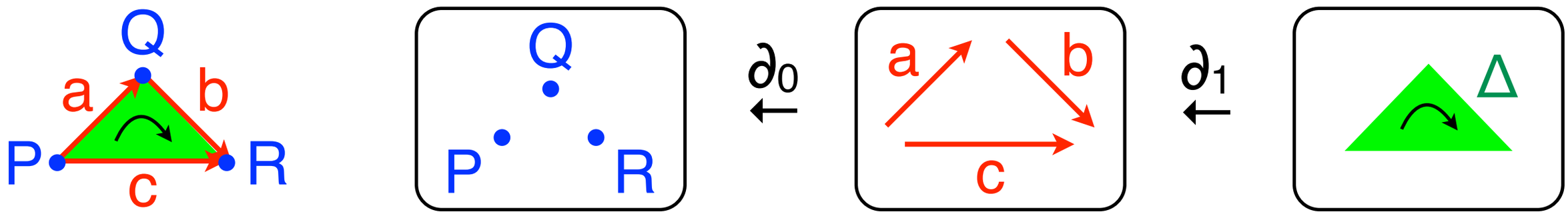
Chain complexes

Definition : A *chain complex* is an infinite sequence

$$C : C_0 \xleftarrow{\partial_0} C_1 \xleftarrow{\partial_1} C_2 \leftarrow \cdots \leftarrow C_n \xleftarrow{\partial_n} C_{n+1} \xleftarrow{\partial_{n+1}} C_{n+2} \leftarrow \cdots$$

of abelian groups such that $\partial_n \, \partial_{n+1} = 0$ for all n.

Example : The *(full) triangle* Δ_2



$\partial_0 a = Q - P$ $\partial_0 b = R - Q$ $\partial_0 c = R - P$ $\partial_1 \Delta = a + b - c$

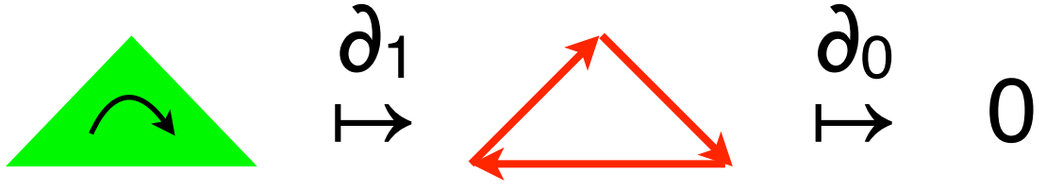
$$\Delta_2 : \mathbb{Z}^3 \xleftarrow{\partial_0} \mathbb{Z}^3 \xleftarrow{\partial_1} \mathbb{Z} \leftarrow 0 \leftarrow 0 \leftarrow \cdots \qquad \partial_0 \, \partial_1 = 0$$

Remark : By removing the 2-cell Δ,
we get the *empty triangle* $\partial\Delta_2$.

Homology of complexes

Let $C : C_0 \xleftarrow{\partial_0} C_1 \xleftarrow{\partial_1} C_2 \leftarrow \cdots \leftarrow C_n \xleftarrow{\partial_n} C_{n+1} \xleftarrow{\partial_{n+1}} C_{n+2} \leftarrow \cdots$

Remark : $\partial_n \, \partial_{n+1} = 0 \Leftrightarrow \text{im } \partial_{n+1} \subset \ker \partial_n$



➔ any *boundary* is a *cycle*

Definition : C is *exact* if $\text{im } \partial_{n+1} = \ker \partial_n$ for all n.

➔ any *cycle* is a *boundary*

Examples : The complex Δ_2 is exact, but not $\partial\Delta_2$.

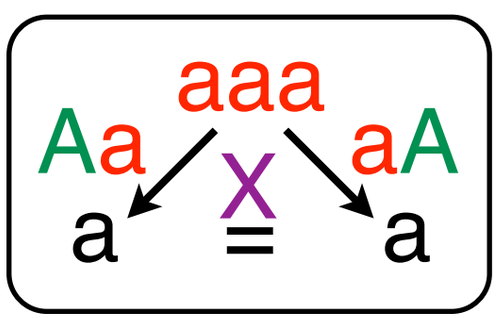
Definition : The *homology groups* of C are
$H_0(C) = C_0 / \text{im } \partial_0 \;\ldots\; H_{n+1}(C) = \ker \partial_n / \text{im } \partial_{n+1}$.

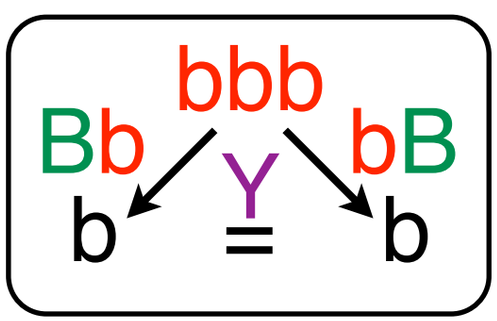
Homology of reductions

Any convergent presentation (Σ,R) defines a complex:

$$\mathbb{Z} \xleftarrow{\partial_0} \mathbb{Z}\cdot\Sigma \xleftarrow{\partial_1} \mathbb{Z}\cdot R \xleftarrow{\partial_2} \mathbb{Z}\cdot P \leftarrow \cdots \qquad \text{with } \partial_0 = 0$$

Exemple : $aa \xrightarrow{A} 1$, $bb \xrightarrow{B} 1$, $aba \xrightarrow{C} bab$

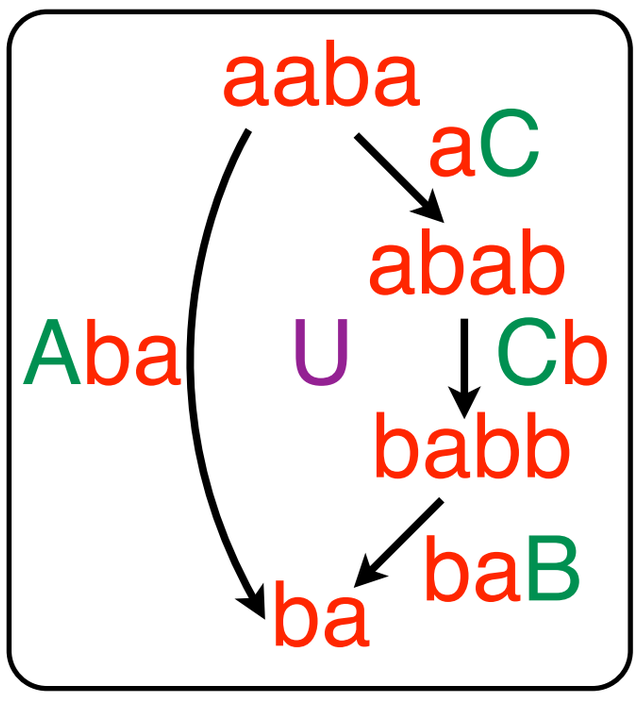


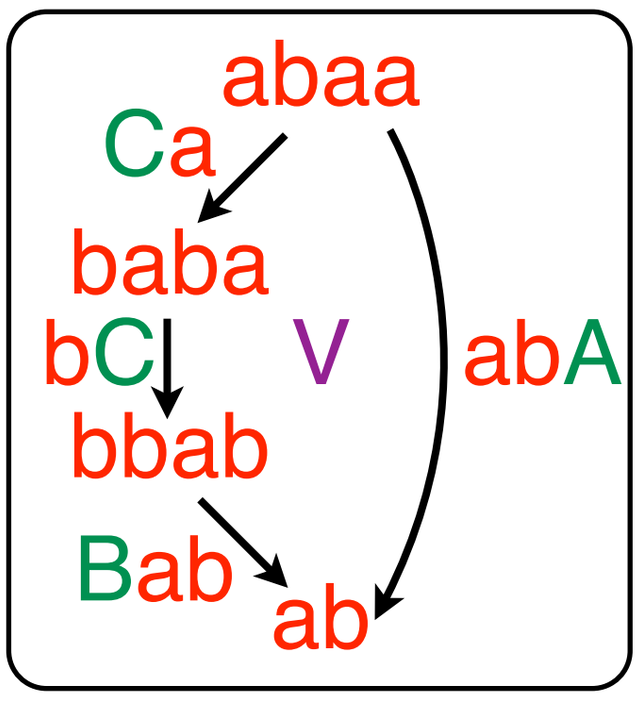


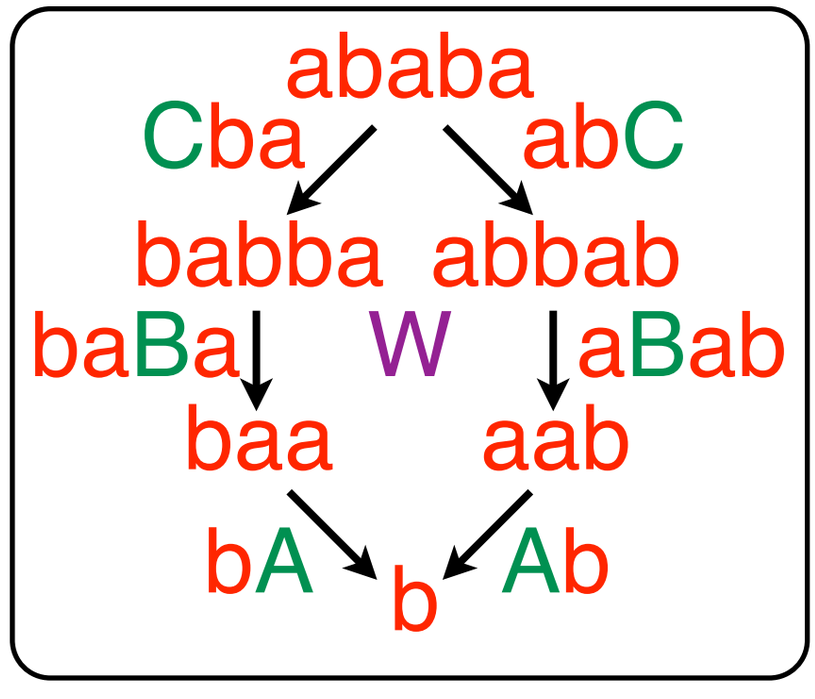
$\partial_1 A = -2a$

$\partial_1 B = -2b$

$\partial_1 C = b - a$







$\partial_2 X = \partial_2 Y = 0$ $\partial_2 U = 2C + B - A$ $\partial_2 V = A - B - 2C$ $\partial_2 W = 0$

Homology of reductions

Theorem (Anick, Squier, Kobayashi) : This homology does not depend on the choice of the (convergent) presentation: it is the *homology of the monoid* $M = \Sigma^*/\leftrightarrow^*_R$.

Corollary (Squier 1987) : If M has a finite convergent presentation, then the abelian group $H_3(M)$ has *finite type*.

In particular, Squier could build a monoid M such that:

- M has a finite presentation (Σ,R),
- the word problem for M is decidable,
- M has no finite convergent presentation.

He proved that the group $H_3(M)$ has infinite type.

Remark : $H_1(M)$, $H_2(M)$ have *finite type* because Σ,R are finite.

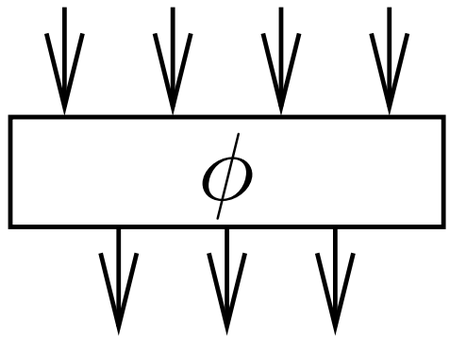
References

- Craig Squier, *Word problems and a homological finiteness condition for monoid* (JPPA 1987)
- Yuji Kobayashi, *Complete rewrite systems and homology of monoid algebras* (JPAA 1990)
- Craig Squier, Friedrich Otto & Yuji Kobayashi, *A finiteness condition for rewriting* system (JPAA 1994)
- Yves Lafont, *Algebra and geometry of rewriting* (ACS 2007)
- Yves Lafont, *Réécriture et problème du mot* (Gazette des mathématiciens, SMF 2009)

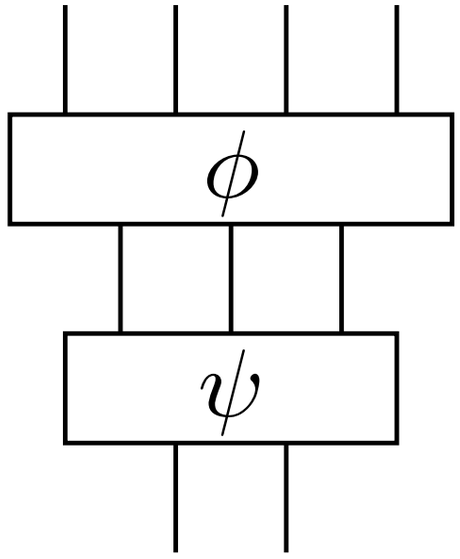
Part 3 : Diagram rewriting

Diagrams

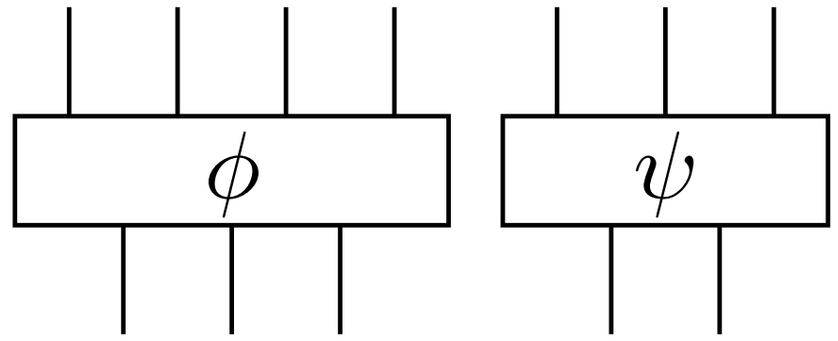
Inputs/outputs



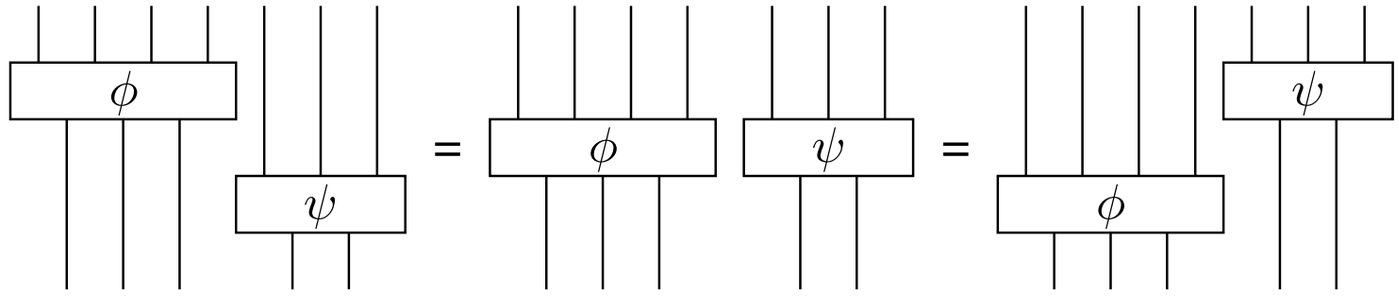
Sequential composition



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)

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

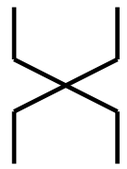
- *linear case*: $\oplus$ (direct sum)

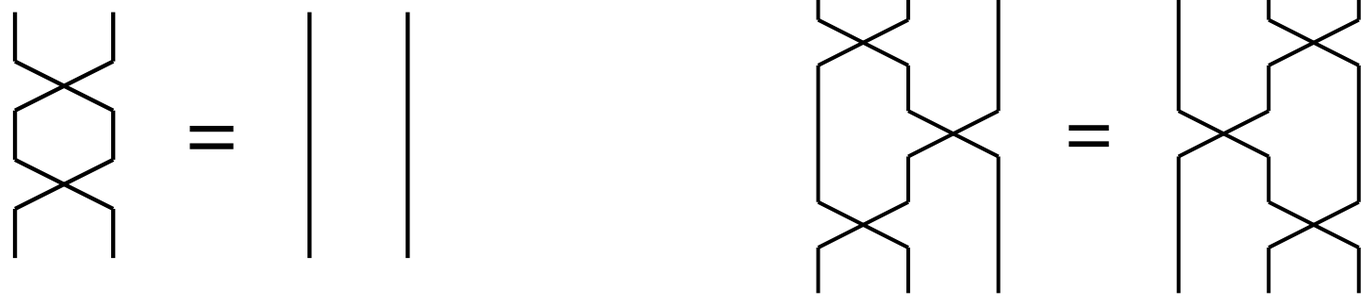
$$f : \mathbb{Z}_2^p \to \mathbb{Z}_2^q \qquad (\mathbb{Z}_2 = \{0,1\},\ \mathbb{Z}_2^p = \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2)$$

- *quantum case*: $\otimes$ (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

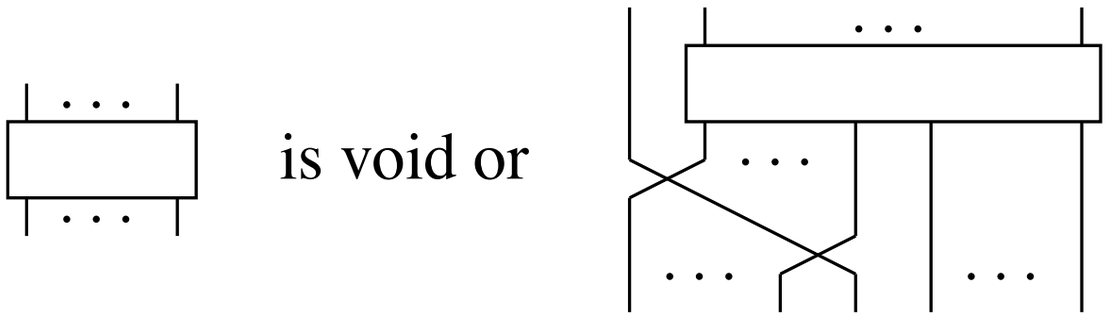
Generator 

Relations 

- Any finite permutation is given by a diagram.
- Two diagrams define the same permutation if and only if they are equivalent modulo the above relations.

Canonical forms

Grammar for canonical forms:

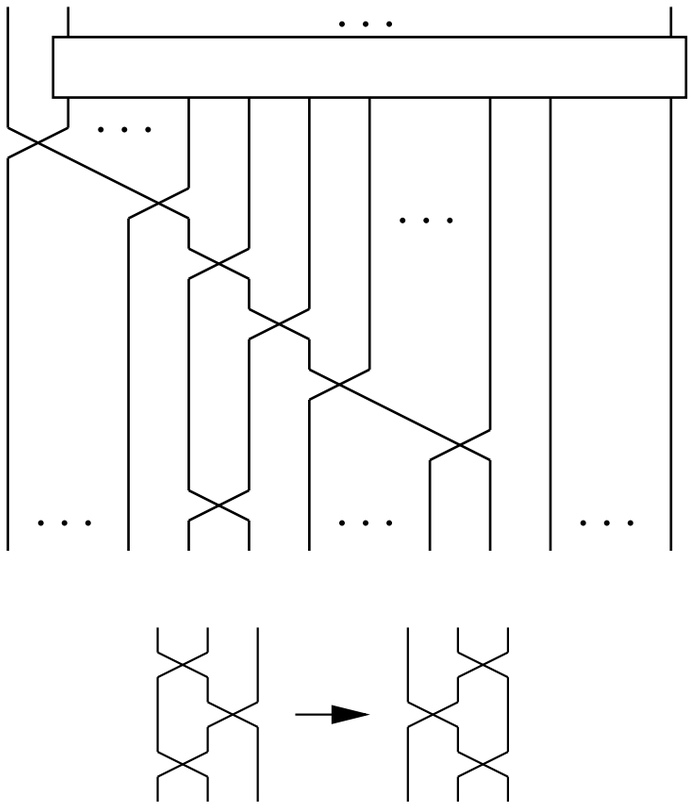


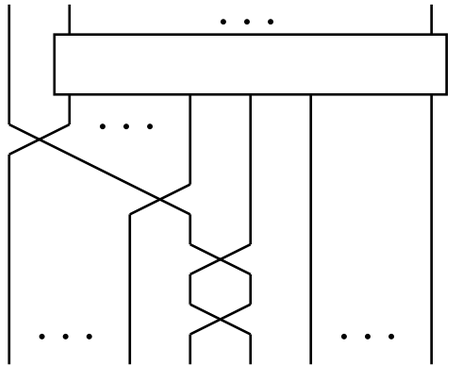
- Any permutation corresponds to a unique *canonical form*.
- Any diagram reduces to a canonical form by the following two *rewrite rules*:

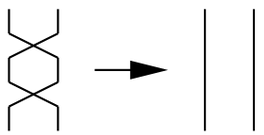
Reduction to the canonical form

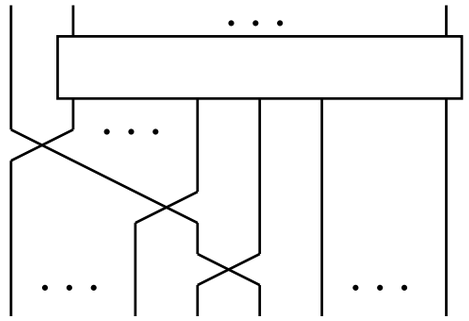
By double induction:

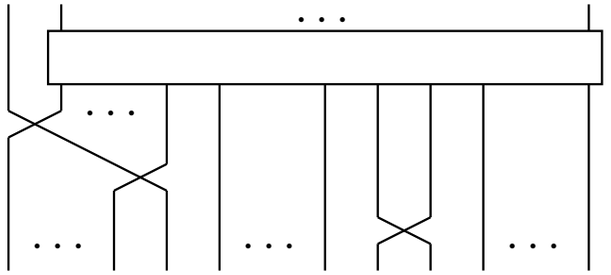
- on the *width* (number of wires)
- on the *size* (total number of gates)





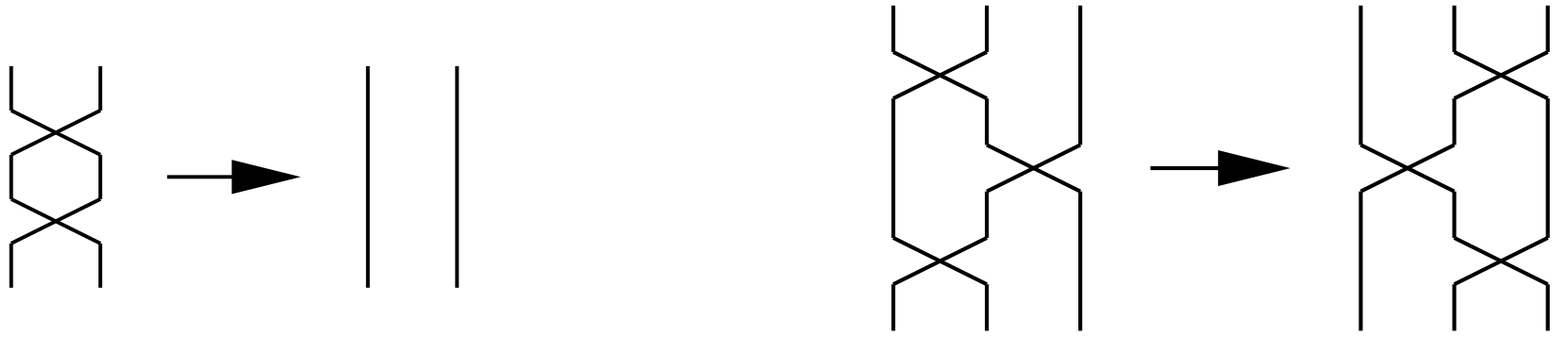






(interchange)

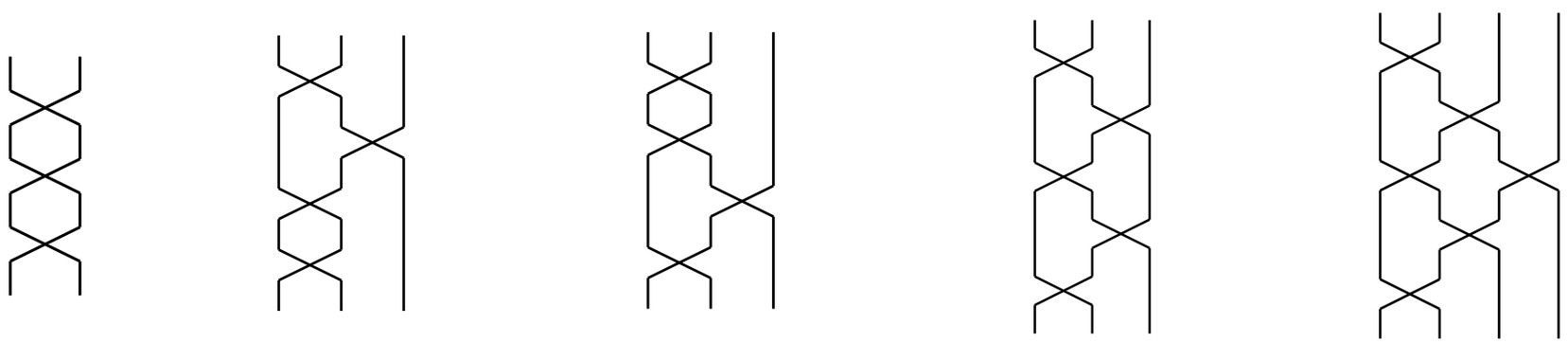
Rewriting



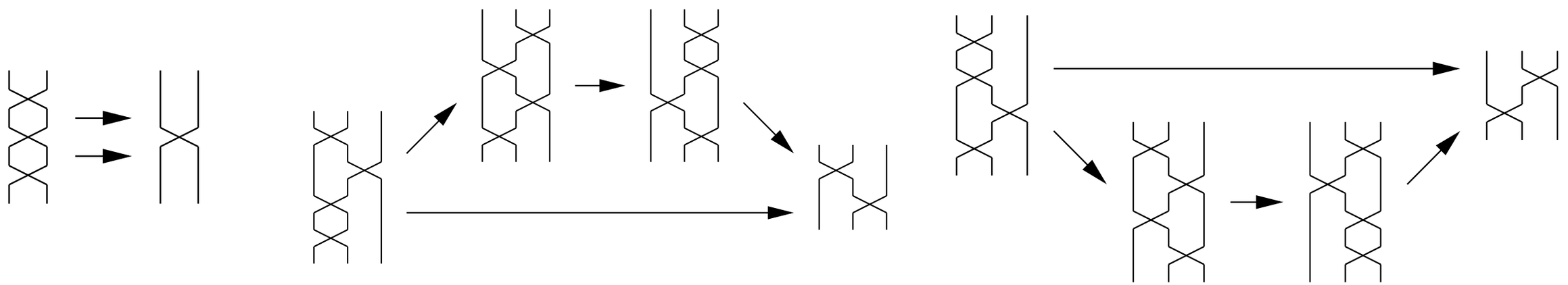
This rewrite system is *convergent*.

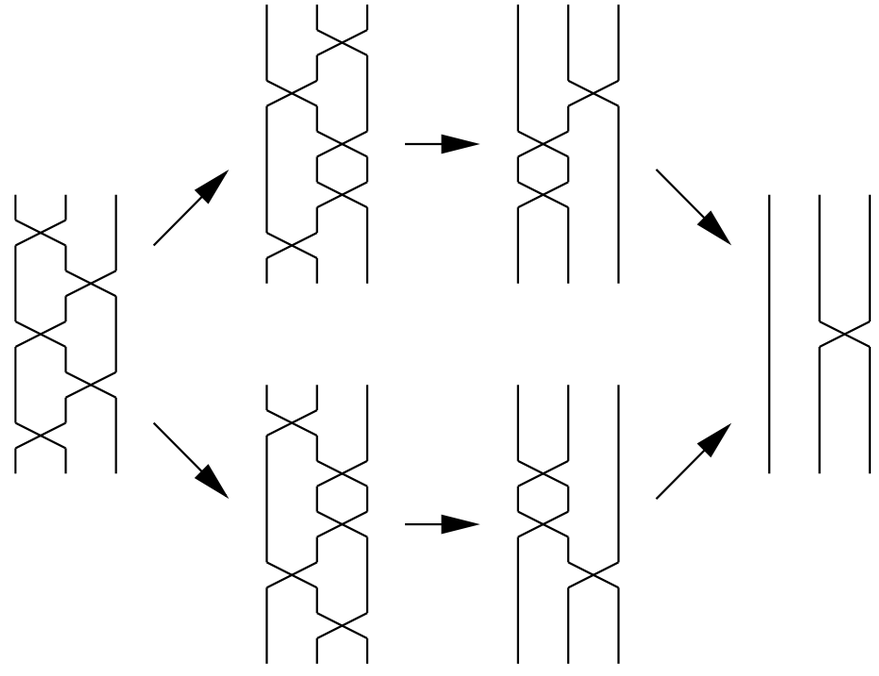
- *Termination* (existence of a canonical form)
- *Confluence* (uniqueness of the canonical form)

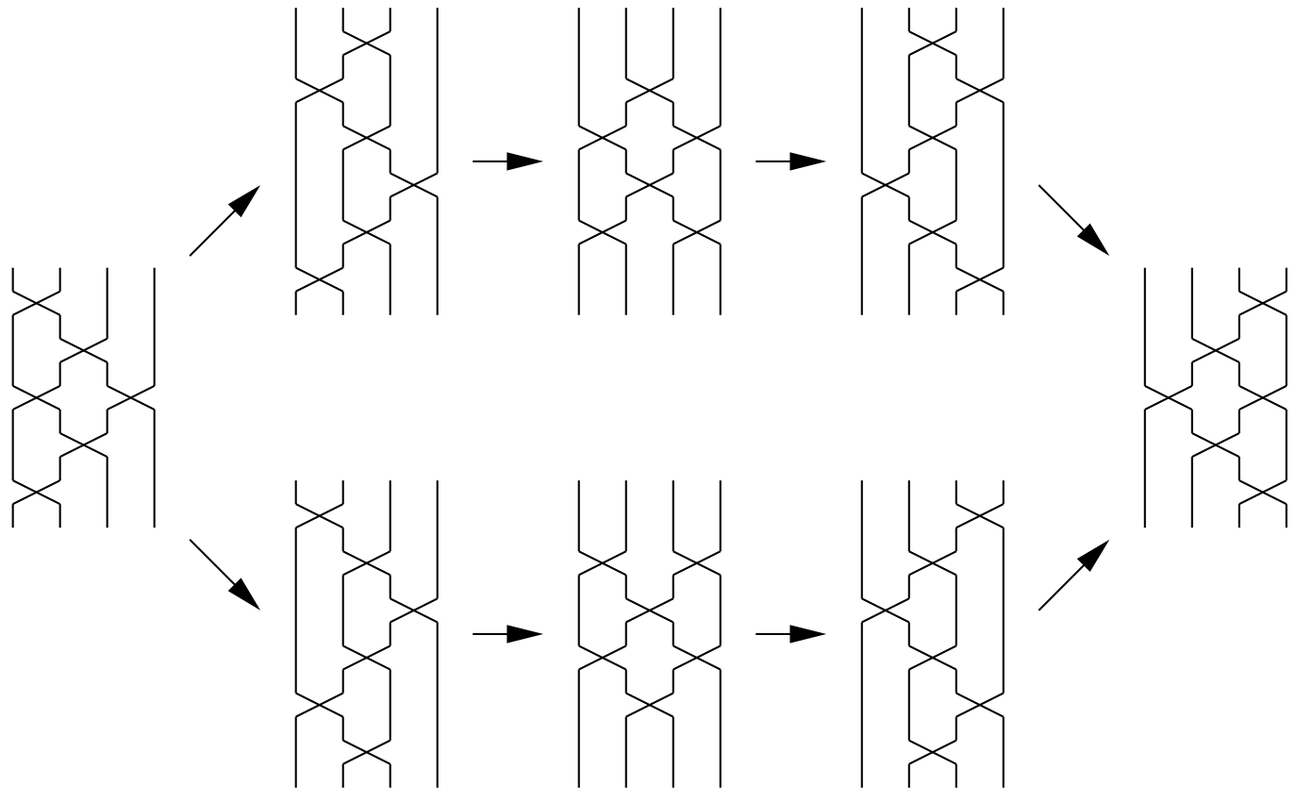
Conflicts (*critical peaks*)



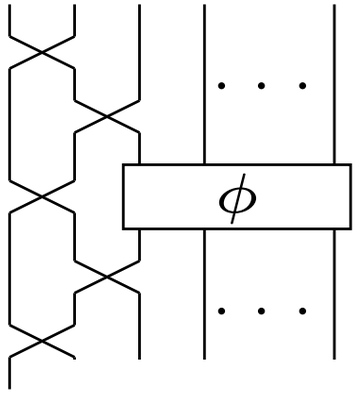
Confluence of critical peaks

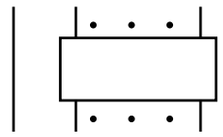
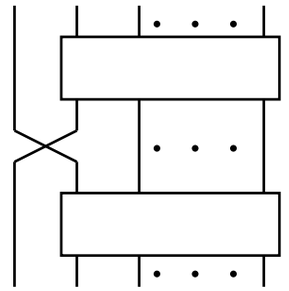




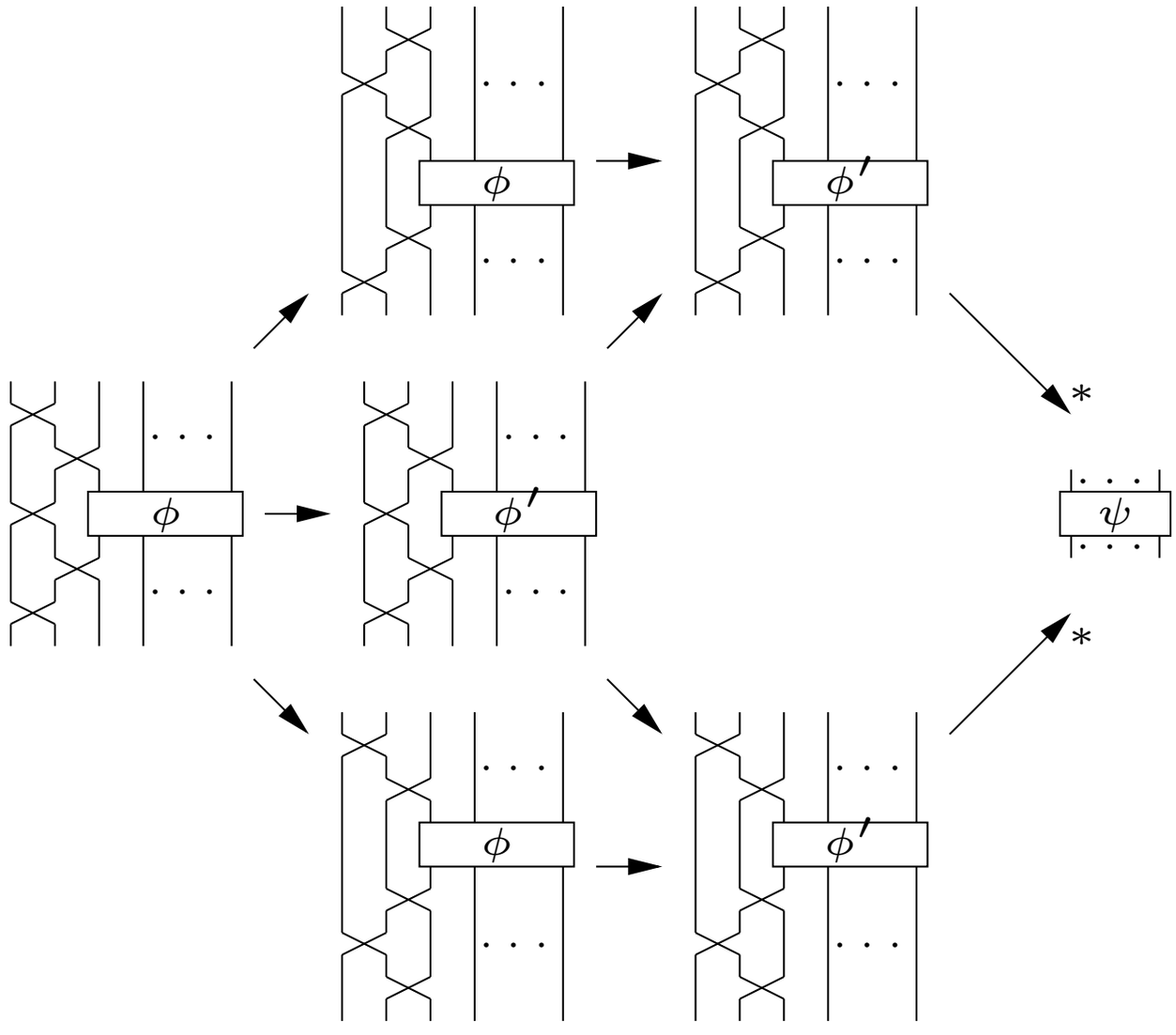


Confluence of global conflicts



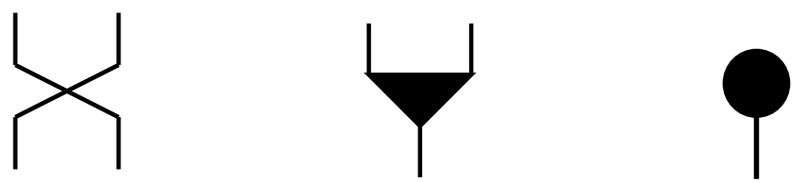
where ϕ is  or 

By induction

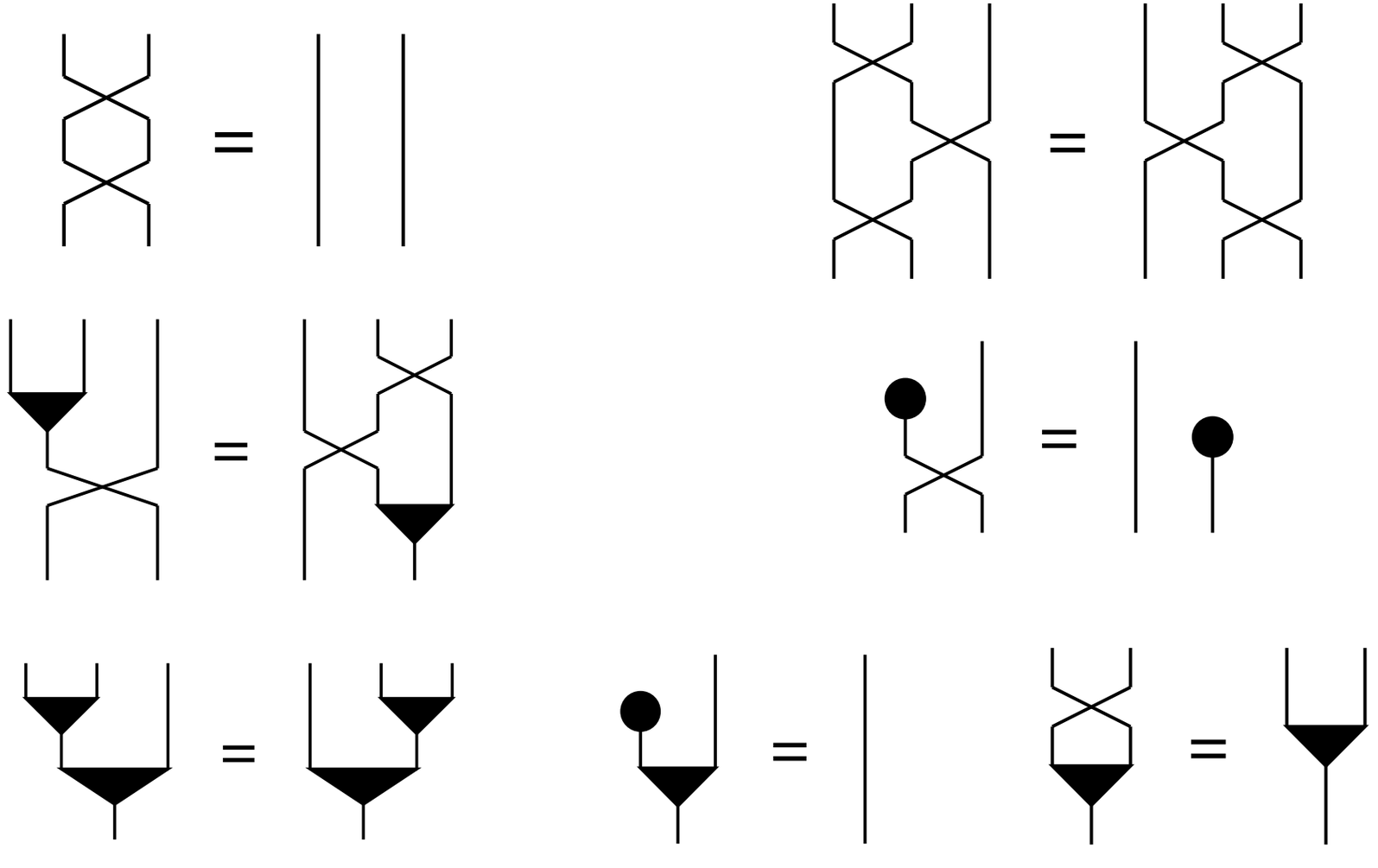


Second example: Finite maps

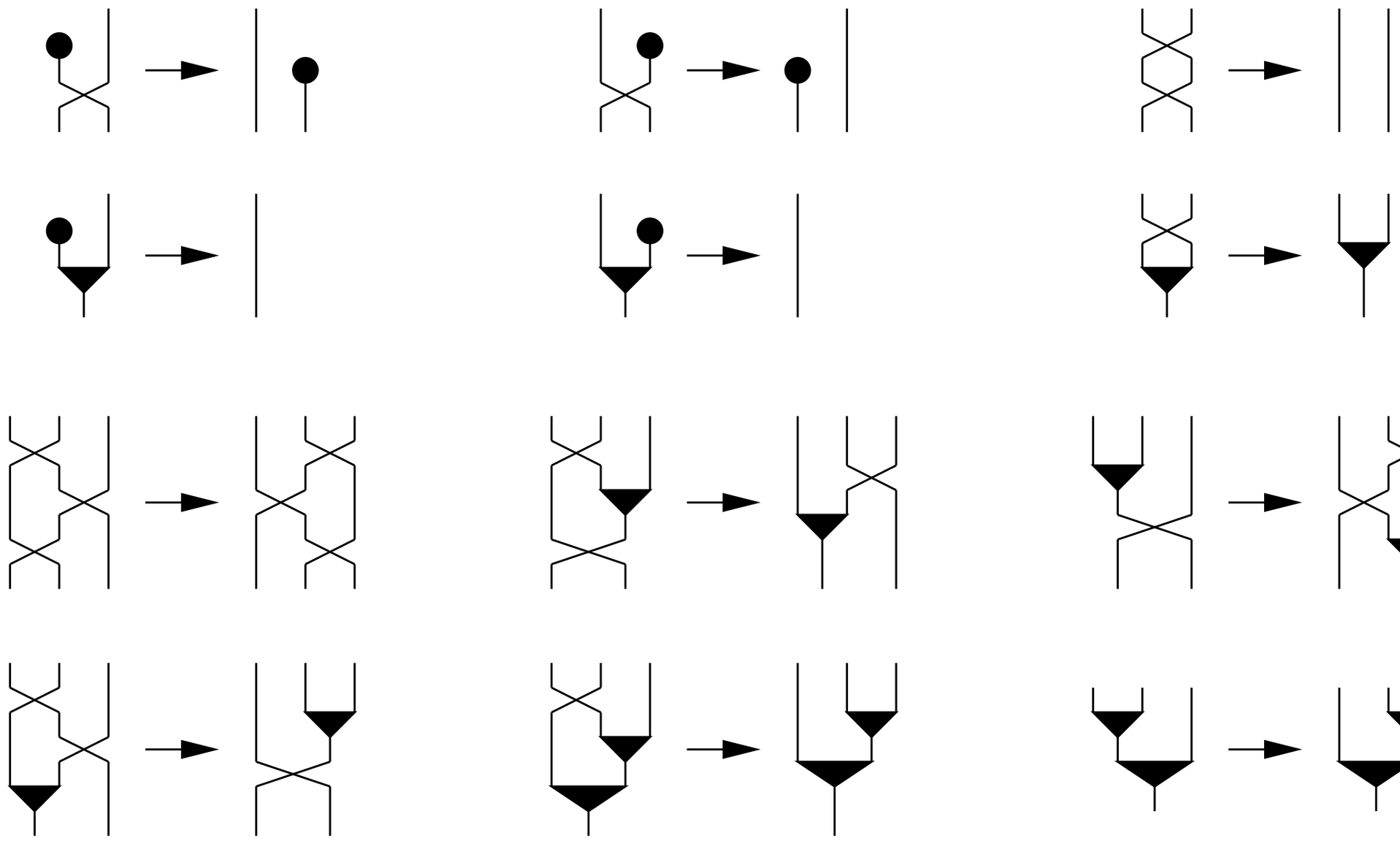
Generators



Relations

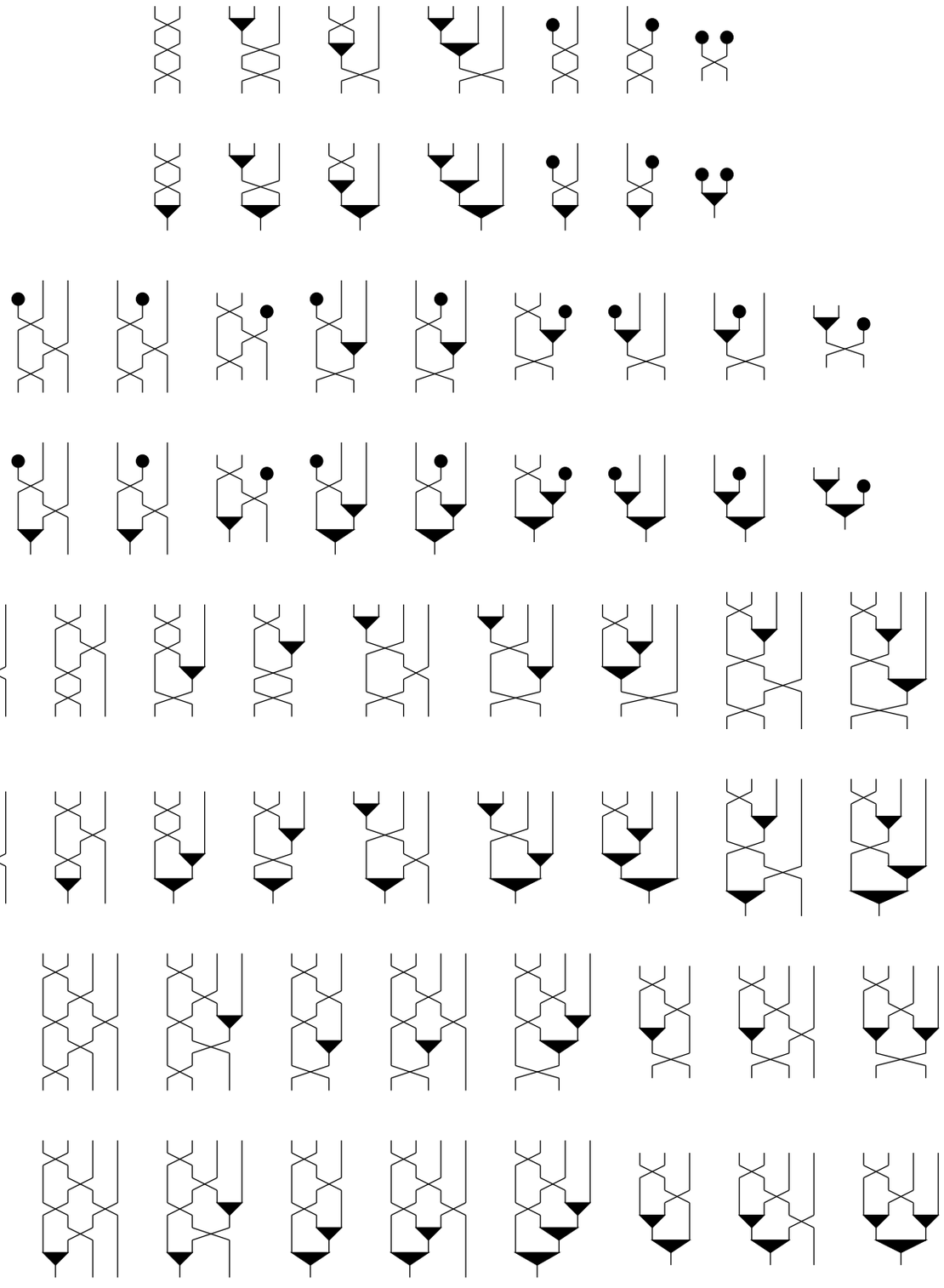


Rewrite rules

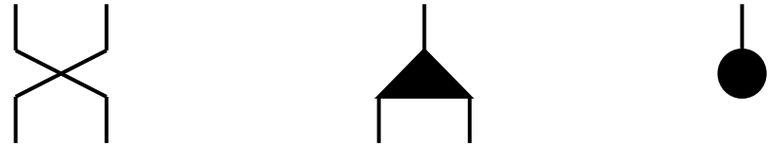


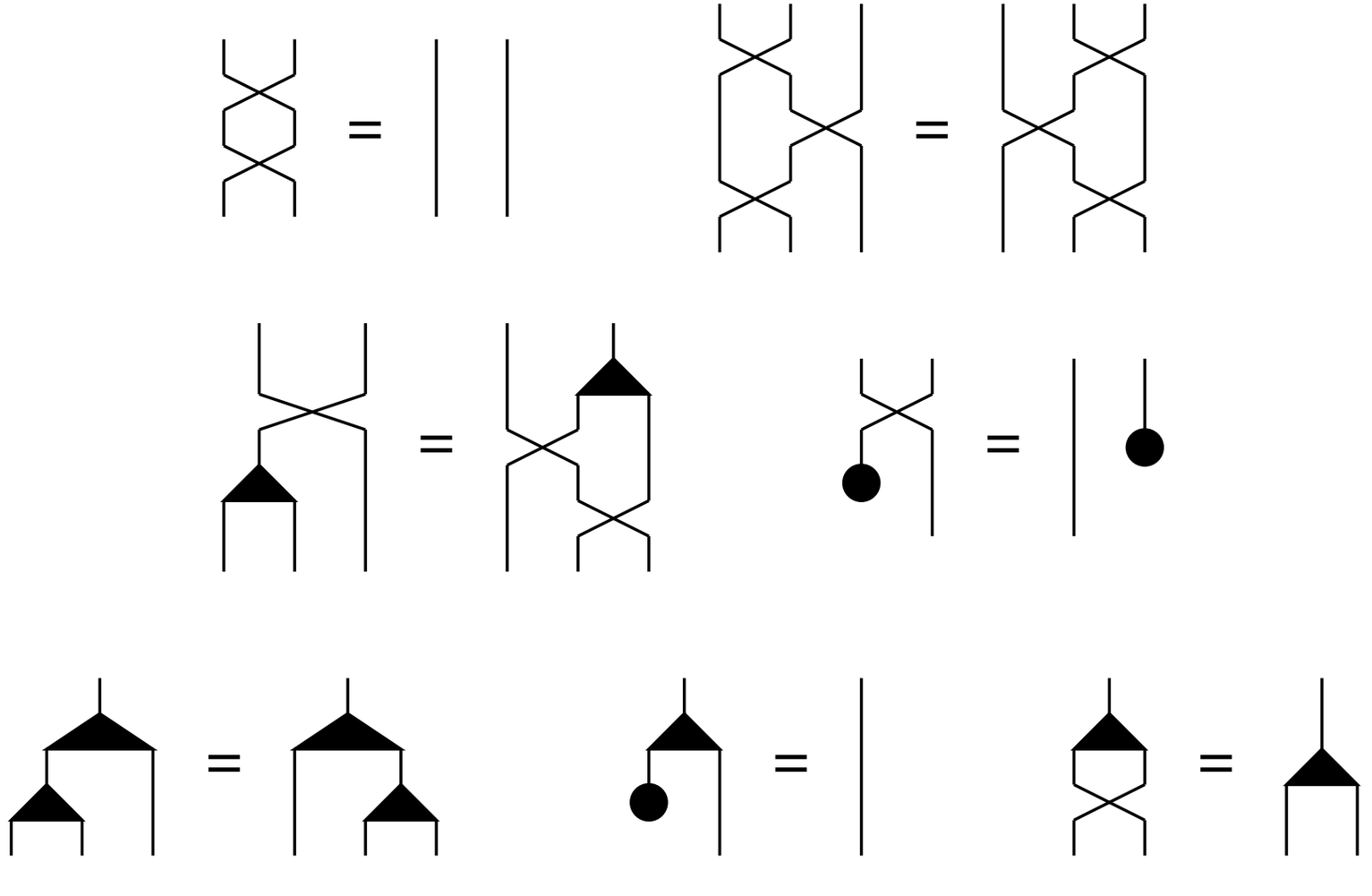
This rewrite system is convergent.

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 91].
    - Any finite convergent left linear rewrite system (with terms) yields a finite convergent rewrite system (with diagrams) [Lafont 95].

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

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 & Pierre Rannou, *Diagram rewriting for orthogonal matrices* (RTA 2008)