HOMOLOGICAL COMPUTATIONS FOR TERM REWRITING SYSTEMS

Philippe Malbos, **Samuel Mimram**
École Polytechnique

FSCD conference

June 22, 2016

Algebraic theories

An **algebraic theory** consists of

1. operations with given arities
2. equations between terms generated by operations

Example

- the theory of groups is given by $m : 2$, $e : 0$, $i : 1$ and

$$m(m(x_1, x_2), x_3) = m(x_1, m(x_2, x_3))$$
$$m(e, x_1) = x_1 \qquad m(x_1, e) = x_1$$
$$m(i(x_1), x_1) = e \qquad m(x_1, i(x_1)) = e$$

- rings, fields, etc.
- (semi)lattices, booleans algebras, etc.

Models

A **model** of an algebraic theory consists of

- a set X
- an interpretation $[\![f]\!] : X^n \to X$
  for each operation f of arity n
- such that the axioms are satisfied

Example

Models of the theory of groups are groups.

Equivalence between theories

Two theories are **equivalent** when they have the same models.

Example

Consider the theory of groups, given by $m : 2$, $e : 0$, $i : 1$ and

$$m(m(x_1, x_2), x_3) = m(x_1, m(x_2, x_3))$$

$$m(e, x_1) = x_1 \qquad\qquad m(x_1, e) = x_1$$

$$m(i(x_1), x_1) = e \qquad\qquad m(x_1, i(x_1)) = e$$

The equations in red are derivable from the other.

Equivalence between theories

Two theories are **equivalent** when they have the same models.

Example

Consider the theory of groups, given by $m : 2$, $e : 0$, $i : 1$ and

$$m(m(x_1, x_2), x_3) = m(x_1, m(x_2, x_3))$$

$$m(e, x_1) = x_1 \qquad\qquad m(x_1, e) = x_1$$

$$m(i(x_1), x_1) = e \qquad\qquad m(x_1, i(x_1)) = e$$

The equations in red are derivable from the other.

$$\begin{aligned} xe &= (ex)e = ((x^{--}x^{-})x)e = (x^{--}(x^{-}x))e = (x^{--}e)e \\ &= x^{--}(ee) = x^{--}e = x^{--}(x^{-}x) = (x^{--}x^{-})x = ex = x \end{aligned}$$

Equivalence between theories

Two theories are **equivalent** when they have the same models.

Example

Consider the theory of groups, given by $m : 2$, $e : 0$, $i : 1$ and

$$\begin{aligned} m(m(x_1, x_2), x_3) &= m(x_1, m(x_2, x_3)) \\ m(e, x_1) &= x_1 \\ m(i(x_1), x_1) &= e \end{aligned}$$

The equations in red are derivable from the other.

$$\begin{aligned} xe &= (ex)e = ((x^{--}x^{-})x)e = (x^{--}(x^{-}x))e = (x^{--}e)e \\ &= x^{--}(ee) = x^{--}e = x^{--}(x^{-}x) = (x^{--}x^{-})x = ex = x \end{aligned}$$

Finding small axiomatizations

Can we find minimal (or small) axiomatizations for theories?

One relation for (abelian) groups

In 1938, Tarski observed that the theory of abelian groups can be axiomatized with two operations $d : 2$, $a : 0$ and one relation

$$d(x_1, d(x_2, d(x_3, d(x_1, x_2)))) = x_3$$

where a ensures that we exclude the empty model.

A **one-based** theory is a theory which can be axiomatized with only one axiom.

The quest for one-based theories

There is an interesting line of efforts to find one-based theories:

- 1938: abelian groups is one-based
- 1952: groups is one-based
- 1965: semi-lattices is not one-based
- 1970: distributive lattices is not one-based
  lattices is one-based (300 000 sym. / 34 var.)
- 1973: boolean algebras is one-based ($\geq$ 40 000 000 symb.)
- 2002: boolean algebras is one-based (12 symb.)
- 2003: lattices is one-based (29 symb. / 8 var.)
- ...

Not one-based theories

We are interested in showing that theories are *not* one-based:

- existing proofs are tricky and specific to particular theories
- they rely on finding counter-examples using some models

Here, instead

- we provide a method which is entirely automatic
- but it does not provide an answer in every case

The general method

Algorithm

1. start from a theory $\mathcal{T}$
2. orient it so that you get a terminating and confluent rewriting system
3. feed it to the computer and compute

$$H_2(\mathcal{T}) \qquad \in \qquad \mathbb{N}$$

4. we know that we need at least $H_2(\mathcal{T})$ relations

The general method

Algorithm

1. start from a theory $\mathcal{T}$
2. orient it so that you get a terminating and confluent rewriting system
3. feed it to the computer and compute

$$H_2(\mathcal{T}) \qquad \in \qquad \mathbb{N}$$

4. we know that we need at least $H_2(\mathcal{T})$ relations

Note that:

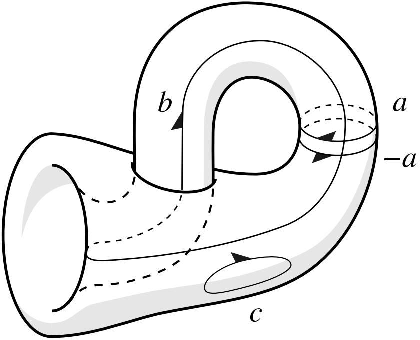
- the theory might not be orientable as a convergent rs
- we might compute $H_2(\mathcal{T}) = 0$
- we have examples where it works though :)

Good!

Let's switch to something else.

Suppose that you have a space (e.g. a simplicial complex) and you want to compute the number of “holes” in it. There is a very efficient way of doing this:

homology



Suppose that our space looks like this:

$$\begin{tikzcd} & y \arrow[dr, "g"] \arrow[d, phantom, "\Uparrow\alpha"] & & \\ x \arrow[ur, "f"] \arrow[rr, "h"'] & {} & z \arrow[r, "i"] & z' \end{tikzcd}$$

Homology

Suppose that our space looks like this:

$$\begin{tikzcd}
 & y \arrow[dr, "g"] & & \\
x \arrow[ur, "f"] \arrow[rr, "h"'] \arrow[rr, phantom, shift left=3ex, "\Uparrow\alpha"] & & z \arrow[r, "i"] & z'
\end{tikzcd}$$

- we allow taking linear combinations of “building blocks”

Homology

Suppose that our space looks like this:

$$\begin{tikzcd}
 & y \arrow[dr, "g"] \arrow[d, phantom, "\Uparrow\alpha"] & & \\
x \arrow[ur, "f"] \arrow[rr, "h"'] & {} & z \arrow[r, "i"] & z'
\end{tikzcd}$$

- we allow taking linear combinations of “building blocks”
- we define the boundary of a block as target - source:

$$\partial(f) = y - x \qquad\qquad \partial(\alpha) = f + g - h$$

Homology

Suppose that our space looks like this:

$$\begin{tikzcd} & y \arrow[dr, "g"] & & \\ x \arrow[ur, "f"] \arrow[rr, "h"'] \arrow[rr, phantom, shift left=4ex, "\Uparrow\alpha"] & & z \arrow[r, "i"] & z' \end{tikzcd}$$

- we allow taking linear combinations of "building blocks"
- we define the boundary of a block as target - source:

$$\partial(f) = y - x \qquad\qquad \partial(\alpha) = f + g - h$$

- "potential holes" can be detected as those with zero boundary:

$$\begin{aligned} \partial(f + g - h) &= \partial(f) + \partial(g) - \partial(h) \\ &= (y - x) + (z - y) - (z - x) = 0 \end{aligned}$$

Homology

Suppose that our space looks like this:

$$
\begin{tikzcd}
 & y \arrow[dr, "g"] & & \\
x \arrow[ur, "f"] \arrow[rr, "h"'] & \arrow[u, phantom, "\Uparrow\alpha"] & z \arrow[r, "i"] & z'
\end{tikzcd}
$$

- we allow taking linear combinations of "building blocks"
- we define the boundary of a block as target - source:

$$\partial(f) = y - x \qquad\qquad \partial(\alpha) = f + g - h$$

- "potential holes" can be detected as those with zero boundary:

$$\begin{aligned}\partial(f + g - h) &= \partial(f) + \partial(g) - \partial(h) \\ &= (y - x) + (z - y) - (z - x) = 0\end{aligned}$$

- we have to remove those that are boundaries

$$\partial(\alpha) = f + g - h$$

Homology

Suppose that our space looks like this:

$$\begin{tikzcd} & y \arrow[dr, "g"] & & \\ x \arrow[ur, "f"] \arrow[rr, "h"'] & & z \arrow[r, "i"] & z' \end{tikzcd}$$

- we allow taking linear combinations of "building blocks"
- we define the boundary of a block as target - source:

$$\partial(f) = y - x \qquad\qquad \partial(\alpha) = f + g - h$$

- "potential holes" can be detected as those with zero boundary:

$$\begin{aligned} \partial(f + g - h) &= \partial(f) + \partial(g) - \partial(h) \\ &= (y - x) + (z - y) - (z - x) = 0 \end{aligned}$$

- we have to remove those that are boundaries

Formally, given our space X:

$$
\begin{tikzcd}
 & y \arrow[dr, "g"] & & \\
x \arrow[ur, "f"] \arrow[rr, "h"'] \arrow[rr, phantom, shift left=3ex, "\Uparrow\alpha"] & & z \arrow[r, "i"] & z'
\end{tikzcd}
$$

we consider the chain complex (i.e. $\partial_{i-1} \circ \partial_i = 0$)

$$
\begin{array}{ccccccc}
\ldots \xrightarrow{\partial_2} & \Bbbk\{\alpha\} & \xrightarrow{\partial_1} & \Bbbk\{f, g, h, i\} & \xrightarrow{\partial_0} & \Bbbk\{x, y, z, z'\} \\
& \| & & \| & & \| \\
& C_2 & & C_1 & & C_0
\end{array}
$$

Homology

Formally, given our space X:

$$\begin{tikzcd} & y \arrow[dr, "g"] & & \\ x \arrow[ur, "f"] \arrow[rr, "h"'] & \Uparrow\alpha & z \arrow[r, "i"] & z' \end{tikzcd}$$

we consider the chain complex (i.e. $\partial_{i-1} \circ \partial_i = 0$)

$$\begin{array}{ccccccc} \ldots \xrightarrow{\partial_2} & \Bbbk\{\alpha\} & \xrightarrow{\partial_1} & \Bbbk\{f, g, h, i\} & \xrightarrow{\partial_0} & \Bbbk\{x, y, z, z'\} \\ & \| & & \| & & \| \\ & C_2 & & C_1 & & C_0 \end{array}$$

and we can compute the i-th homology groups:

$$H_i(X) \quad = \quad \ker \partial_{i+1} / \operatorname{im} \partial_i$$

The intuition is that the rank of $H_i(X)$ counts the number of "holes" in dimension i.

Homology

The i-th homology group is defined by

$$H_i(X) \quad = \quad \ker \partial_{i+1} / \operatorname{im} \partial_i$$

with

$$\partial_i \quad : \quad C_{i+1} \quad \to \quad C_i$$

In particular, we have that

$$\dim(C_i) \quad \geq \quad \dim(H_i(X))$$

i.e.

$$C_i \quad = \quad \mathbb{k}\{x_1, \ldots, x_n\}$$

with

$$n \quad \geq \quad \dim(H_i(X))$$

A theory as a space

Suppose that we can see a theory $\mathcal{T}$ as a "space" with

- points: $\mathbb{N}$
- edges: operations
- surfaces: relations
- volumes: relations between relations (e.g. critical pairs)

$$
\begin{tikzcd}
2 \arrow[rr, bend left=40, "m(x_1,m(i(x_2),x_2))"] \arrow[rr, "m(x_1,e)" description] \arrow[rr, bend right=40, "e"'] \arrow[rr, phantom, shift left=4, "||"] \arrow[rr, phantom, shift right=4, "||"] & & 1
\end{tikzcd}
$$

then

$$\dim(H_2(\mathcal{T}))$$

is a lower bound on the number of relations!

An example

Consider the term rewriting system with generators

$$f:2 \qquad g:2 \qquad a:0 \qquad b:0 \qquad c:0$$

together with rules

$$\begin{array}{lclclcl} A & : & f(a,x_1) \Rightarrow g(a,x_1) & \quad & A' & : & f(x_1,a) \Rightarrow g(x_1,a) \\ B & : & f(b,b) \Rightarrow g(b,b) & \quad & C & : & f(c,c) \Rightarrow g(c,c) \end{array}$$

An example

Consider the term rewriting system with generators

$$f : 2 \qquad g : 2 \qquad a : 0 \qquad b : 0 \qquad c : 0$$

together with rules

$$\begin{array}{lclclcl} A & : & f(a, x_1) \Rightarrow g(a, x_1) & \quad & A' & : & f(x_1, a) \Rightarrow g(x_1, a) \\ B & : & f(b, b) \Rightarrow g(b, b) & \quad & C & : & f(c, c) \Rightarrow g(c, c) \end{array}$$

It is terminating with one confluent critical pair

$$\begin{tikzcd} f(a, a) \arrow[rr, Rightarrow, bend left, "A\langle a\rangle"] \arrow[rr, Rightarrow, bend right, "A'\langle a\rangle"'] \arrow[rr, phantom, "\Downarrow\Phi"] & & g(a, a) \end{tikzcd}$$

An example

Note that all the rules

$$\begin{array}{lclclcl} A & : & f(a,x_1) \Rightarrow g(a,x_1) & \quad & A' & : & f(x_1,a) \Rightarrow g(x_1,a) \\ B & : & f(b,b) \Rightarrow g(b,b) & & C & : & f(c,c) \Rightarrow g(c,c) \end{array}$$

have the same "balance":

$$\partial_1(A) \quad = \quad g + a - f - a \quad = \quad g - f$$

An example

Note that all the rules

$$\begin{array}{lcl@{\qquad}lcl} A & : & f(a, x_1) \Rightarrow g(a, x_1) & A' & : & f(x_1, a) \Rightarrow g(x_1, a) \\ B & : & f(b, b) \Rightarrow g(b, b) & C & : & f(c, c) \Rightarrow g(c, c) \end{array}$$

have the same "balance":

$$\begin{array}{lclclcl} \partial_1(A) & = & g + a - f - a & = & g - f & & \\ & = & \partial_1(A') & = & \partial_1(B) & = & \partial_1(C) \end{array}$$

An example

Note that all the rules

$$
\begin{array}{lclclcl}
A & : & f(a,x_1) \Rightarrow g(a,x_1) & A' & : & f(x_1,a) \Rightarrow g(x_1,a) \\
B & : & f(b,b) \Rightarrow g(b,b) & C & : & f(c,c) \Rightarrow g(c,c)
\end{array}
$$

have the same "balance":

$$
\begin{array}{lclclclcl}
\partial_1(A) & = & g+a-f-a & = & g-f & & \\
 & = & \partial_1(A') & = & \partial_1(B) & = & \partial_1(C)
\end{array}
$$

so that we have

$$
\begin{array}{rclcl}
\partial_1(A'-A) & = & \partial_1(A')-\partial_1(A) & = & 0 \\
\partial_1(B-A) & = & \partial_1(B)-\partial_1(A) & = & 0 \\
\partial_1(C-A) & = & \partial_1(C)-\partial_1(A) & = & 0
\end{array}
$$

i.e. there are 3 "potential holes".

An example

Similarly, the "balance" of the critical pair

$$\begin{tikzcd} f(a,a) \arrow[r, bend left, Rightarrow, "A\langle a \rangle"] \arrow[r, bend right, Rightarrow, "A'\langle a \rangle"'] \arrow[r, phantom, "\Downarrow\Phi"] & g(a,a) \end{tikzcd}$$

is

$$\partial_2(\Phi) \quad = \quad A' - A$$

An example

Similarly, the "balance" of the critical pair

$$\begin{tikzcd} f(a,a) \arrow[rr, Rightarrow, bend left, "A\langle a\rangle"] \arrow[rr, Rightarrow, bend right, "A'\langle a\rangle"'] \arrow[rr, phantom, "\Downarrow\Phi"] & & g(a,a) \end{tikzcd}$$

is

$$\partial_2(\Phi) \quad = \quad A' - A$$

Therefore, we have in fact two holes:

$$\cancel{A' - A} \qquad\qquad B - A \qquad\qquad C - A$$

An example

Similarly, the "balance" of the critical pair

$$
\begin{tikzcd}
f(a,a) \arrow[rr, Rightarrow, bend left, "A\langle a \rangle"] \arrow[rr, Rightarrow, bend right, "A'\langle a \rangle"'] \arrow[rr, phantom, "\Downarrow\Phi"] & & g(a,a)
\end{tikzcd}
$$

is

$$\partial_2(\Phi) \quad = \quad A' - A$$

Therefore, we have in fact two holes:

$$\cancel{A' - A} \qquad\qquad B - A \qquad\qquad C - A$$

The vector space generated by these two holes is a subspace of the one generated by rules

$$H_2(\mathcal{T}) \qquad \subseteq \qquad C_2$$

and therefore we need at least to rules to present the theory.

Invariance under axiomatization

Why do we need to use such tools?

- A fundamental property of homology is that it is invariant under weak equivalences (= deformations of spaces)
- In the setting of theories, this will translate as

  homology is invariant under the axiomatization

  i.e. we have bounds on *any* axiomatization of the theory
- This is where we need the assumption that we have a convergent rewriting system!

HOMOLOGY OF LAWVERE THEORIES

Lawvere theories

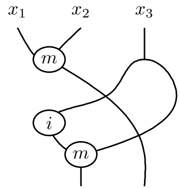
All the operations described by a Lawvere theory can be encoded into a category called a **Lawvere theory**:

- objects: natural numbers
- morphisms $m \to n$: n-uples of terms with variables in $\{x_1, \ldots, x_m\}$ up to the relations
- composition: substitution

Example

In the theory of groups, we have the morphism

$$\langle \quad m(i(x_3), x_3) \quad , \quad m(x_1, x_2) \quad \rangle \quad : \quad 3 \to 2$$



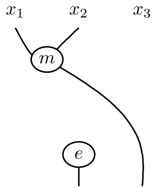
All the operations described by a Lawvere theory can be encoded into a category called a **Lawvere theory**:

- objects: natural numbers
- morphisms $m \to n$: n-uples of terms with variables in $\{x_1, \ldots, x_m\}$ up to the relations
- composition: substitution

Example

In the theory of groups, we have the morphism

$$\langle \quad e \quad , \quad m(x_1, x_2) \quad \rangle \quad : \quad 3 \to 2$$



Lawvere theories

All the operations described by a Lawvere theory can be encoded into a category called a **Lawvere theory**:

- objects: natural numbers
- morphisms $m \to n$: n-uples of terms with variables in $\{x_1, \dots, x_m\}$ up to the relations
- composition: substitution

Remark

The notion of equivalence can be changed from

- having the same models

to

- generating the same Lawvere theory

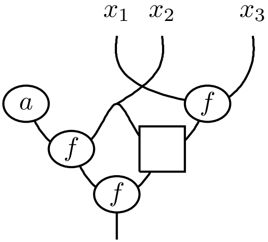
So, the question is:

given a Lawvere theory $\mathcal{T}$, how do we define and compute $H_i(\mathcal{T})$?

Contexts

A **context** is a term with one "inside hole" $\square$.

For instance $\quad f(f(a, x_2), \square(x_2, f(x_1, x_3)))$



of type

$$2 \quad \to \quad 3$$

We write $\mathcal{K}$ for the category of bicontexts.

The ringoid of contexts

A **ringoid** $\mathcal{R}$ is a category enriched in **Ab**:

- each $\mathcal{C}(A, B)$ has a structure of abelian group
- the expected compatibility laws hold:

$$\begin{aligned} (g + g') \circ (f + f') &= g \circ f + g \circ f' + g' \circ f + g' \circ f' \\ 0 \circ f &= 0 \\ f \circ 0 &= 0 \end{aligned}$$

We write $\mathbb{Z}\mathcal{K}$ for the **free ringoid over contexts**, *modulo the rules*.

The ringoid of contexts

We write $\mathbb{Z}\mathcal{K}$ for the **free ringoid over contexts**, *modulo the rules*: the rules have to be "linearized" in order to ensure that $\square$ occurs once.

Example

For instance, the relation $f(x_1) \Rightarrow g(x_1, x_1)$ induces the relation

$$g(\square, x_1) + g(x_1, \square) - f(\square)$$

on contexts.

Modules

A **module** over $\mathbb{Z}\mathcal{K}$ is an **Ab**-enriched functor

$$\mathcal{M} \quad : \quad \mathbb{Z}\mathcal{K} \quad \to \quad \mathbf{Ab}$$

This means that we have things that

- we can add
- we can put into a context

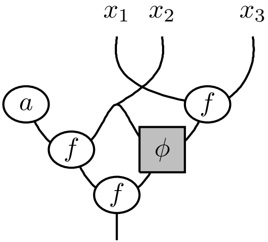
Given a context $K : m \to n$ and a "term" $t \in \mathcal{M}(m)$, we write

$$K[t] \quad = \quad \mathcal{M}(K)(t)$$

Free modules

Given a family $(X_n)_{n\in\mathbb{N}}$ of sets, whose elements are "n-ary things", we can form the **free $\mathbb{Z}\mathcal{K}$-module** $\mathbb{Z}\mathcal{K}\underline{X_n}$.

For instance, we have



with $\phi \in X_2$.

The trivial module

We define the **trivial $\mathbb{Z}\mathcal{K}$-module**

$$\mathcal{Z}$$

with one operation in each arity.

Resolutions

Suppose given a theory $\mathcal{T}$ presented by a convergent algebraic theory (= term rewriting system) with

- P_1 as rules
- P_2 as relations
- P_3 as critical pairs

Theorem (MM16)

We have a partial free resolution, i.e. a complex

$$\mathbb{Z}\mathcal{K}\underline{P_3} \xrightarrow{\partial_2} \mathbb{Z}\mathcal{K}\underline{P_2} \xrightarrow{\partial_1} \mathbb{Z}\mathcal{K}\underline{P_1} \xrightarrow{\partial_0} \mathbb{Z}\mathcal{K}\underline{1} \xrightarrow{\partial_{-1}} \mathcal{Z} \longrightarrow 0$$

of $\mathcal{Z}$ by $\mathbb{Z}\mathcal{K}$-modules where

- *the ∂_i are $\mathbb{Z}\mathcal{K}$-linear maps defined from source and target*
- $\operatorname{im} \partial_i = \ker \partial_{i-1}$

Face maps

The face maps $\partial_i : \mathbb{Z}\mathcal{K}\mathsf{P}_{i+1} \to \mathbb{Z}\mathcal{K}\mathsf{P}_i$ are defined by

$$\text{“target”} \quad - \quad \text{“source”}$$

e.g. for each rule $R : t \Rightarrow u$ we have

$$\partial_1(\underline{R}) \quad = \quad \underline{u} - \underline{t}$$

Homology

We define the **homology** (with trivial coefficients) of the theory $\mathcal{T}$ as the homology of the deduced chain complex obtained by "erasing" $\mathbb{Z}\mathcal{K}$:

$$\mathbb{Z}\mathcal{K}\,\underline{P_3} \xrightarrow{\partial_2} \mathbb{Z}\mathcal{K}\,\underline{P_2} \xrightarrow{\partial_1} \mathbb{Z}\mathcal{K}\,\underline{P_1} \xrightarrow{\partial_0} \mathbb{Z}\mathcal{K}\underline{1} \xrightarrow{\partial_{-1}} \mathcal{Z} \longrightarrow 0$$

$$\rightsquigarrow$$

$$P_3 \xrightarrow{\partial_2'} \quad P_2 \xrightarrow{\partial_1'} \quad P_1 \xrightarrow{\partial_0'} \quad 1$$

and compute

$$H_i(\mathcal{T}) \quad = \quad \ker \partial_{i-1}' / \operatorname{im} \partial_i'$$

Invariance

Theorem (classical)

The homology only depends on $\mathcal{T}$: if we started from another presentation we would have obtained the same homology.

Proof.

Between any two resolutions there is essentially one morphisms. Therefore any two deduced chain complexes (by "erasing" $\mathbb{Z}\mathcal{K}$) are isomorphic and in particular the homologies are isomorphic. $\square$

CONCLUSION

Conclusion

- we presented a generic method to compute lower bounds on generators / relations of a presentation of an algebraic theory
- it can serve to generate simple counter-examples
- it suggests considering higher-dimensional invariants
- most of the "usual" theories are out of reach for now ($H_i(\mathcal{T}) = 0$, commutativity, etc.)
- it suggests new research tracks in algebraic topology