HIGHER-ORDER REWRITING SYSTEMS, CATEGORIAL ALGEBRAS, AND CURRY-HOWARD ISOMORPHISMS

Yangzhou University
Yangzhou, 2025

Enric Cosme Llópez

Departament de Matemàtiques
Universitat de València
School of Mathematics and Statistics
Nantong University

REFERENCES

J. Climent Vidal, E. Cosme Llópez. **From higher-order rewriting systems to higher-order categorial algebras and higher-order Curry-Howard isomorphisms**. ArXiv, abs/2402.12051, 2024.

Mathematics are **written**.
To calculate is to **rewrite**.

REWRITING SYSTEM

A **rewriting system** is an ordered tuple $\boldsymbol{\mathcal{A}} = (\Sigma, X, \mathcal{A})$ where

- Σ is a signature;
- X is a set of variables;
- $\mathcal{A}$ is a subset of $\mathrm{T}_\Sigma(X)^2$.

The elements of $\mathcal{A}$ are called **rewriting rules**.

PATHS

A **path in $\mathcal{A}$** of length $m \in \mathbb{N}$ is

$$\mathfrak{P} = ((P_i)_{i \in m+1}, (\mathfrak{p}_i)_{i \in m}, (T_i)_{i \in m})$$

where, for every $i \in m$, if $\mathfrak{p}_i = (M_i, N_i)$, then

(1) $T_i(M_i) = P_i$; (2) $T_i(N_i) = P_{i+1}$.

$$\mathfrak{P}\colon\ P_0 \xrightarrow{(\mathfrak{p}_0, T_0)} P_1 \xrightarrow{(\mathfrak{p}_1, T_1)} \cdots \xrightarrow{(\mathfrak{p}_{m-2}, T_{m-2})} P_{m-1} \xrightarrow{(\mathfrak{p}_{m-1}, T_{m-1})} P_m$$

PATHS

Example

$$\mathfrak{P}:\ \oplus(x, \oplus(x, y)) \xrightarrow{((y,z),\ \oplus(x,\oplus(x,\_)))} \oplus(x, \oplus(x, z)) \xrightarrow{((\oplus(x,z),z),\ \oplus(x,\_))} \oplus(x, z) \xrightarrow{((\oplus(x,z),\odot(\boxdot(z,x),z,\boxdot(x,x))),\ \_)} \odot(\boxdot(z, x), z, \boxdot(x, x)) \xrightarrow{((z,x),\ \odot(\boxdot(z,x),\_,\boxdot(x,x)))} \odot(\boxdot(z, x), x, \boxdot(x, x)) \xrightarrow{((\boxdot(z,x),y),\ \odot(\_,x,\boxdot(x,x)))} \odot(y, x, \boxdot(x, x)) \xrightarrow{((\boxdot(x,x),z),\ \odot(y,x,\_))} \odot(y, x, z) \xrightarrow{((\odot(y,x,z),\top),\ \_)} \top$$

PATHS

Word problem

In $G = \langle a, b \mid ab = ba \rangle$

$$\begin{aligned} babb^{-1}ab^{-1} &= baab^{-1} \\ &= abab^{-1} \\ &= a^2bb^{-1} \\ &= a^2. \end{aligned}$$

PATHS

Elementary transformations

$$\begin{bmatrix} 2 & 2 & 18 \\ 2 & 3 & 23 \\ 0 & 2 & 11 \end{bmatrix} \xrightarrow{r_1 = \frac{1}{2} r_1} \begin{bmatrix} 1 & 1 & 9 \\ 2 & 3 & 23 \\ 0 & 2 & 11 \end{bmatrix}$$

$$\xrightarrow{r_2 = r_2 - 2 r_1} \begin{bmatrix} 1 & 1 & 9 \\ 0 & 1 & 5 \\ 0 & 2 & 11 \end{bmatrix}$$

$$\xrightarrow{r_3 = r_3 - 2 r_2} \begin{bmatrix} 1 & 1 & 9 \\ 0 & 1 & 5 \\ 0 & 0 & 1 \end{bmatrix}$$

PATHS

Derivatives

$$\begin{aligned}\frac{\partial}{\partial x}\left[\cos(x^2+x)\right] &= (-\sin(x^2+x))\frac{\partial}{\partial x}\left[x^2+x\right] \\ &= -\sin(x^2+x)\left(\frac{\partial}{\partial x}\left[x^2\right]+\frac{\partial}{\partial x}\left[x\right]\right) \\ &= -\sin(x^2+x)(2x+1).\end{aligned}$$

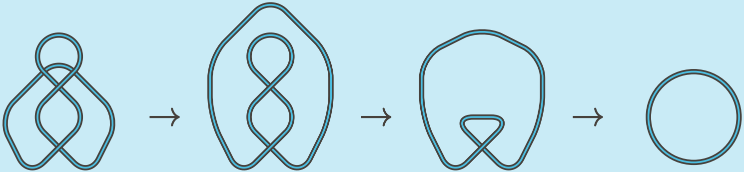
PATHS

Proof by Natural Deduction

$$\dfrac{P \lor Q \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[P]}{[\neg Q]}}{P \qquad \neg P}}{\bot}}{\neg\neg Q}}{Q}}{P \to Q} \qquad \dfrac{\dfrac{[Q]}{Q}}{Q \to Q}}{Q}$$

PATHS

Reidemeister moves



MAIN QUESTION

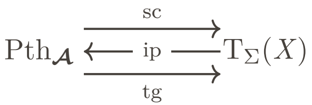
Under what conditions can two rewriting systems be considered **equivalent**?

COMPOSITION

Paths can be composed.

If $\mathfrak{P} \colon P \longrightarrow Q$ and $\mathfrak{Q} \colon Q \longrightarrow R$, then $\mathfrak{Q} \circ \mathfrak{P} \colon P \longrightarrow R$.

Composition is a partial binary operation.



We denote by $\mathbf{Pth}_{\mathcal{A}}$ to the category whose objects are terms and whose morphisms are paths.

DECOMPOSITION

Paths can be decomposed.

If $\mathfrak{p} = (M, N)$ is a rewriting rule in $\mathcal{A}$, its associated **echelon** is the path of length 1

$$\mathrm{Ech}(\mathfrak{p}) : M \xrightarrow{(\mathfrak{p},\_)} N$$

We will say that a path has echelons if any of its subpaths of length 1 is an echelon.

DECOMPOSITION

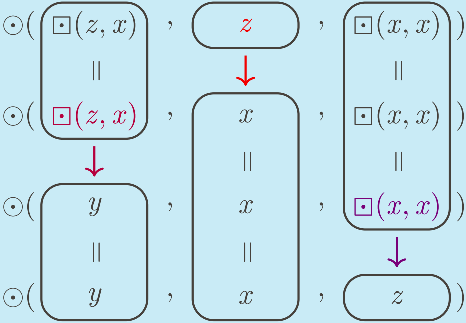
Example

$$
\begin{array}{rcl}
\mathfrak{P}:\ \oplus(x, \oplus(x, y)) & \to & \oplus(x, \oplus(x, z)) \\
 & \to & \oplus(x, z) \\
\text{echelon} & \to & \odot(\boxdot(z, x), z, \boxdot(x, x)) \\
 & \to & \odot(\boxdot(z, x), x, \boxdot(x, x)) \\
 & \to & \odot(y, x, \boxdot(x, x)) \\
 & \to & \odot(y, x, z) \\
\text{echelon} & \to & \top
\end{array}
$$

Proposition. Paths without echelons are paths between complex and homogeneous terms.

DECOMPOSITION

Example



Proposition. In a path without echelons, we can extract as many subpaths as the arity of the operation.

DECOMPOSITION

Let $\prec$ be the binary relation on $\mathrm{Pth}_{\boldsymbol{\mathcal{A}}}$ defined by $\mathfrak{Q} \prec \mathfrak{P}$ if

i. $\mathfrak{P}$ has length strictly greater than 1, has its first echelon in position i and $\mathfrak{Q}$ is the prefix subpath strictly preceding the echelon or the suffix subpath containing the echelon; or

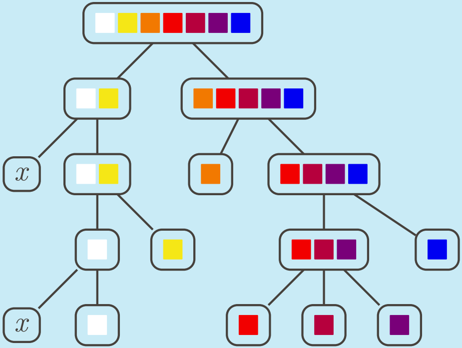
ii. $\mathfrak{P}$ is a non-identity echelonless path and $\mathfrak{Q}$ is one of the subpaths extracted from $\mathfrak{P}$.

We denote by $\leq$ to the reflexive transitive closure of $\prec$.

Proposition. $\leq$ is an Artinian order on $\mathrm{Pth}_{\boldsymbol{\mathcal{A}}}$ whose minimal elements are identity paths and echelons.

DECOMPOSITION

Example



CATEGORIAL SIGNATURE

We define the **categorial signature** determined by the rewriting system $\boldsymbol{\mathcal{A}}$ to be the signature that enlarges Σ with

i. the rewriting rules in $\mathcal{A}$ as constants;
ii. two unary operations sc and tg;
iii. a binary operation $\circ$.

We will denote this signature with $\Sigma^{\boldsymbol{\mathcal{A}}}$.

THE CURRY-HOWARD MAPPING

The Curry-Howard mapping is defined by **Artinian recursion**

$$\mathrm{CH}\colon \mathrm{Pth}_{\boldsymbol{\mathcal{A}}} \longrightarrow \mathrm{T}_{\Sigma^{\boldsymbol{\mathcal{A}}}}(X)$$

1. For minimal paths

$$\mathrm{CH}(\mathrm{ip}(P)) = P; \qquad \mathrm{CH}(\mathrm{Ech}(\mathfrak{p})) = \mathfrak{p}.$$

2. For non-minimal paths

$$\mathrm{CH}(\mathfrak{P}) = \begin{cases} \mathrm{CH}(\mathfrak{P}^{i,|\mathfrak{P}|-1}) \circ \mathrm{CH}(\mathfrak{P}^{0,i-1}); \\ \sigma((\mathrm{CH}(\mathfrak{Q}_j))_{j\in n}). \end{cases}$$

THE CURRY-HOWARD MAPPING

Example

$$
\begin{aligned}
\mathfrak{P}:\ \oplus(x, \oplus(x, y)) &\rightarrow \oplus(x, \oplus(x, z)) \\
&\rightarrow \oplus(x, z) \\
&\rightarrow \odot(\boxdot(z, x), z, \boxdot(x, x)) \\
&\rightarrow \odot(\boxdot(z, x), x, \boxdot(x, x)) \\
&\rightarrow \odot(y, x, \boxdot(x, x)) \\
&\rightarrow \odot(y, x, z) \\
&\rightarrow \top
\end{aligned}
$$

$$
\mathrm{CH}(\mathfrak{P}) = (({\color{blue}\blacksquare} \circ (\odot({\color{purple}\blacksquare}, {\color{red}\blacksquare}, {\color{violet}\blacksquare}))) \circ {\color{orange}\blacksquare}) \circ (\oplus(x, {\color{yellow}\blacksquare} \circ \oplus(x, {\color{lightgray}\blacksquare})))
$$

THE ALGEBRA OF PATHS

Proposition. The set $\mathrm{Pth}_{\boldsymbol{\mathcal{A}}}$ has structure of partial $\Sigma^{\boldsymbol{\mathcal{A}}}$-algebra, that we will denote by $\mathbf{Pth}_{\boldsymbol{\mathcal{A}}}$, where the operations are given by

$$\mathbf{sc}(\mathfrak{P}) = \mathrm{ip}(\mathrm{sc}(\mathfrak{P})); \qquad \mathbf{tg}(\mathfrak{P}) = \mathrm{ip}(\mathrm{tg}(\mathfrak{P}));$$

$$\boldsymbol{\mathfrak{p}} = \mathrm{Ech}(\mathfrak{p}); \qquad \mathfrak{Q} \mathbin{\boldsymbol{\circ}} \mathfrak{P} = \mathfrak{Q} \circ \mathfrak{P}.$$

THE ALGEBRA OF PATHS

If $\sigma \in \Sigma_n$ and $(\mathfrak{P}_j)_{j\in n} \in \mathrm{Pth}^n_{\boldsymbol{\mathcal{A}}}$, then

$$\boldsymbol{\sigma}((\mathfrak{P}_j)_{j\in n}) : \begin{array}{cccccccc}
\sigma(& \mathrm{sc}(\mathfrak{P}_0) & , & \mathrm{sc}(\mathfrak{P}_1) & , & \cdots & , & \mathrm{sc}(\mathfrak{P}_{n-1})) \\
 & \downarrow \mathfrak{P}_0 & & \| & & & & \| \\
\sigma(& \mathrm{tg}(\mathfrak{P}_0) & , & \mathrm{sc}(\mathfrak{P}_1) & , & \cdots & , & \vdots\ ) \\
 & \| & & \downarrow \mathfrak{P}_1 & & & & \| \\
\sigma(& \vdots & , & \mathrm{tg}(\mathfrak{P}_1) & , & \ddots & , & \mathrm{sc}(\mathfrak{P}_{n-1})) \\
 & \| & & \| & & & & \downarrow \mathfrak{P}_{n-1} \\
\sigma(& \mathrm{tg}(\mathfrak{P}_0) & , & \mathrm{tg}(\mathfrak{P}_1) & , & \cdots & , & \mathrm{tg}(\mathfrak{P}_{n-1}))
\end{array}$$

Proposition. $\sigma((\mathfrak{P}_j)_{j\in n})$ is an echelonless path.

THE KERNEL OF THE CURRY-HOWARD MAPPING

Proposition. CH is a Σ-homomorphism but not necessarily a $\Sigma^{\mathcal{A}}$-homomorphism.

$$\mathrm{CH}(\mathrm{ip}(P)) = \mathrm{CH}(\mathrm{ip}(P) \circ \mathrm{ip}(P)) \neq \mathrm{CH}(\mathrm{ip}(P)) \circ \mathrm{CH}(\mathrm{ip}(P)).$$

Proposition. $\mathrm{Ker}(\mathrm{CH})$ is a closed $\Sigma^{\mathcal{A}}$-congruence.

The quotient $\mathrm{Pth}_{\mathcal{A}}/\mathrm{Ker}(\mathrm{CH})$ will be denoted by $[\mathrm{Pth}_{\mathcal{A}}]$ and the class of a path $\mathfrak{P}$ will be denoted by $[\mathfrak{P}]$.

THE QUOTIENT OF PATHS

The quotient $[\mathrm{Pth}_{\boldsymbol{\mathcal{A}}}]$ has structure of **partial $\Sigma^{\boldsymbol{\mathcal{A}}}$-algebra, partially ordered set, and category**.

Furthermore, the operations $\sigma \in \Sigma$ of arity n are **functors** from $[\mathrm{Pth}_{\boldsymbol{\mathcal{A}}}]^n$ to $[\mathrm{Pth}_{\boldsymbol{\mathcal{A}}}]$, since

$$\mathbf{sc}\left(\sigma\left(([\mathfrak{P}_j])_{j\in n}\right)\right) = \sigma\left((\mathbf{sc}([\mathfrak{P}_j]))_{j\in n}\right)$$
$$\mathbf{tg}\left(\sigma\left(([\mathfrak{P}_j])_{j\in n}\right)\right) = \sigma\left((\mathbf{tg}([\mathfrak{P}_j]))_{j\in n}\right)$$
$$\sigma\left(([\mathfrak{Q}_j] \circ [\mathfrak{P}_j])_{j\in n}\right) = \sigma\left(([\mathfrak{Q}_j])_{j\in n}\right) \circ \sigma\left(([\mathfrak{P}_j])_{j\in n}\right)$$

This is a **categorial Σ-algebra** that we denote it by $[\mathbf{Pth}_{\boldsymbol{\mathcal{A}}}]$.

THE QUOTIENT OF PATHS

Theorem. The quotient $[\mathbf{Pth}_{\mathcal{A}}]$ is the free partial $\Sigma^{\mathcal{A}}$-algebra generated by $\mathbf{Pth}_{\mathcal{A}}$ for a variety of partial $\Sigma^{\mathcal{A}}$-algebras $\mathbf{PAlg}(\mathcal{E}^{\mathcal{A}})$.

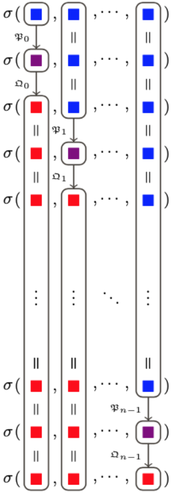
Equations relative to the categorical structure.

Existence of productions.

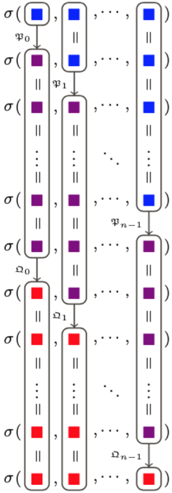
Relationship between the operations and the composition.

$$\left[\bigwedge_{j\in n}(x_j \circ y_j \stackrel{\mathrm{e}}{=} x_j \circ y_j)\right] \to \sigma((x_j \circ y_j)_{j\in n}) \stackrel{\mathrm{e}}{=} \sigma((x_j)_{j\in n}) \circ \sigma((y_j)_{j\in n}).$$

THE QUOTIENT OF PATHS



$\sigma((\mathfrak{Q}_j \circ \mathfrak{P}_j)_{j \in n})$



$\sigma((\mathfrak{Q}_j)_{j \in n}) \circ \sigma((\mathfrak{P}_j)_{j \in n})$

A CURRY-HOWARD RESULT

Theorem. There exists a pair of inverse mappings

$$[\mathbf{Pth}_{\mathcal{A}}] \underset{\mathrm{ip}^{\mathrm{fc}}}{\overset{\mathrm{CH}}{\rightleftarrows}} [\mathbf{PT}_{\mathcal{A}}] \quad (\cong)$$

- isomorphisms of partial $\Sigma^{\mathcal{A}}$-algebras;
- order isomorphisms;
- isomorphisms of categories.

HIGHER-ORDER

> **Algebra is the offer made by the devil to the mathematician. The devil says: I will give you this powerful machine, it will answer any question you like. All you need to do is give me your soul. Give up geometry and you will have this marvellous machine.**
>
> —M. Atiyah.

SECOND-ORDER REWRITING SYSTEMS

This process can be **iterated**.

1. We introduce the notion of first-order translation T.
2. For every term class $[M] \in [\mathrm{PT}_{\mathcal{A}}]$, and every $M' \in [M]$.

$$[T(M)] = [T(M')].$$

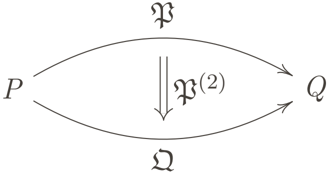
3. We introduce the notion of second-order rewriting rules as pairs $\mathfrak{p}^{(2)} = ([M],[N])$ with the condition

$$\mathrm{sc}\left(\mathrm{ip}^{\mathrm{fc}}(M)\right) = \mathrm{sc}\left(\mathrm{ip}^{\mathrm{fc}}(N)\right); \quad \mathrm{tg}\left(\mathrm{ip}^{\mathrm{fc}}(M)\right) = \mathrm{tg}\left(\mathrm{ip}^{\mathrm{fc}}(N)\right).$$

4. We introduce the notion of **second-order paths**.

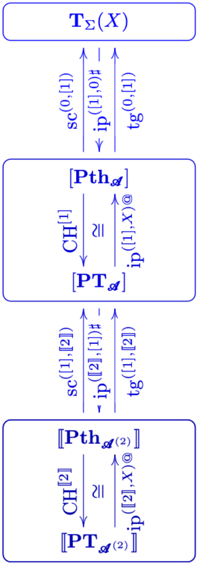
SECOND-ORDER PATHS

A second-order path $\mathfrak{P}^{(2)}$ has the form

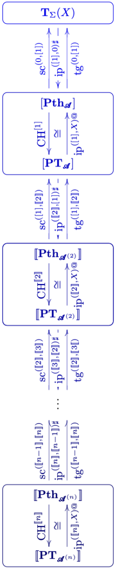


Mutatis mutandis **we recover the previous results**.

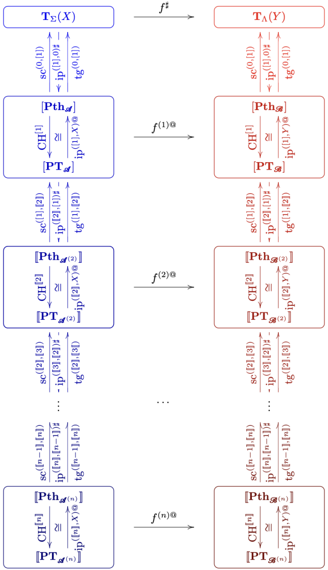
SECOND-ORDER RESULTS



N-TH ORDER RESULTS



SIMULATION MORPHISMS



SIMULATION MORPHISMS

To determine a **simulation morphism** from $\boldsymbol{\mathcal{A}}^{(n)}$ to $\boldsymbol{\mathcal{B}}^{(n)}$ we will assign

- to every variable in X a term in $\mathrm{T}_{\Gamma}(Y)$
- to every operation in Σ a **derived operation** in $\mathrm{T}_{\Gamma}(Y)$
- to every k-th rewriting rule in $\mathcal{A}^{(k)}$ a k-th order path in $\mathrm{Pth}_{\boldsymbol{\mathcal{B}}^{(k)}}$ respecting sources and targets

The final mapping $f^{(k)@} \colon [\![\mathbf{Pth}_{\boldsymbol{\mathcal{A}}^{(k)}}]\!] \longrightarrow [\![\mathbf{Pth}_{\boldsymbol{\mathcal{B}}^{(k)}}]\!]$, is obtained by **Artinian recursion** and by **universal property** on the quotients.

FUTURE WORK

1. Towers of rewriting systems.
2. Projective limits of rewriting systems.
3. Classifying spaces.
4. Fundamental grupoids.

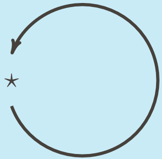
SYNTHETIC TOPOLOGY

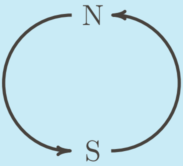
In these days the angel of topology and the devil of abstract algebra fight for the soul of every individual discipline of mathematics.

—H. Weyl.

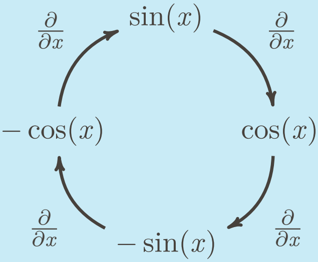
Two rewriting systems

$$\mathbb{S}^1 = \begin{cases} X & = & \{\star\} \\ \Sigma & = & \varnothing \\ \mathcal{A} & = & \{(\star, \star)\} \end{cases} \qquad \mathrm{S}\mathbb{I} = \begin{cases} Y & = & \{\mathrm{N}, \mathrm{S}\} \\ \Gamma & = & \varnothing \\ \mathcal{B} & = & \{(\mathrm{N}, \mathrm{S}), (\mathrm{S}, \mathrm{N})\} \end{cases}$$



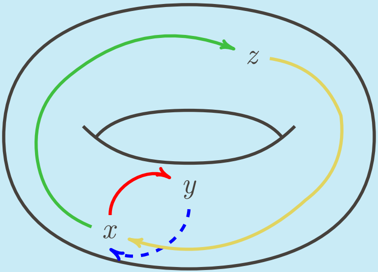


A simulation for the $\mathbb{S}^1$

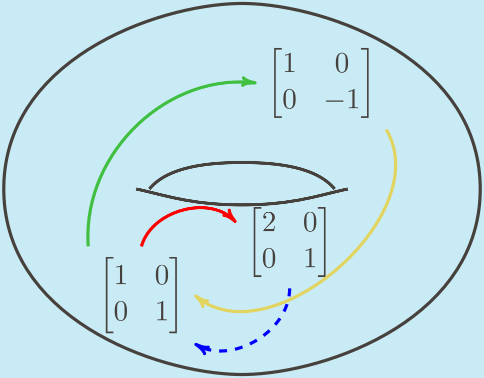


An specification for $\mathbb{T}^2$

$$\mathbb{T}^2 = \begin{cases} X & = & \{x, y, z\} \\ \Sigma & = & \varnothing \\ \mathcal{A} & = & \{\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \mathfrak{s}\} \\ \mathcal{A}^{(2)} & = & \{((\mathfrak{s} \circ \mathfrak{r}) \circ (\mathfrak{q} \circ \mathfrak{p}), (\mathfrak{q} \circ \mathfrak{p}) \circ (\mathfrak{s} \circ \mathfrak{r}))\} \end{cases}$$



A simulation of the $\mathbb{T}^2$



$$(-f_2 \circ -f_2) \circ (\tfrac{1}{2} f_1 \circ 2 f_1) = (\tfrac{1}{2} f_1 \circ 2 f_1) \circ (-f_2 \circ -f_2)$$

What if we could prove **topological properties** using rewriting systems?

- $\mathbb{T}^2 \cong \mathbb{S}^1 \times \mathbb{S}^1$.
- $\pi_1\left(\mathbb{T}^2\right) = \mathbb{Z} \oplus \mathbb{Z}$.
- $\mathbb{T}^2$ is orientable.
- $\ldots$

La possibilité de la traduction implique l'existence d'un invariant. Traduire, c'est précisément dégager cet invariant.

—H. Poincaré.

Thanks!