Nominal sets for quantum memory

An algebraic account of linear parameters

Pierre Cagne

Laboratoire PPS, Université Paris Diderot

October 7, 2015

1

Nominal sets

Definitions

Let A be a infinite countable set of *variables*.

Denote $\mathfrak{S}_A$ for the permutation group of A.
A $\mathfrak{S}_A$-set is a set together with an action of $\mathfrak{S}_A$.

Definitions

Let A be a infinite countable set of *variables*.

Denote $\mathfrak{S}_A$ for the permutation group of A.
A $\mathfrak{S}_A$-set is a set together with an action of $\mathfrak{S}_A$.

Support

An element x of a $\mathfrak{S}_A$-set X has support $S \subseteq A$ if for every $\sigma \in \mathfrak{S}_A$,

$$(\forall s \in S, \sigma s = s) \implies \sigma \cdot x = x$$

Remark: the set of supports of a element is closed by supset.

Definitions

Let A be a infinite countable set of *variables*.

Denote $\mathfrak{S}_A$ for the permutation group c
A $\mathfrak{S}_A$-set is a set together with an actio

$A = \{x_1, x_2, \dots\}$
$X = \{\lambda\text{-terms over } A\}$
Action: $\sigma \cdot t = t[x_i/\sigma(x_i)]$

t has support S iff $S \supseteq \mathrm{FV}(t)$

Support

An element x of a $\mathfrak{S}_A$-set X has support $S \subseteq A$ if for every $\sigma \in \mathfrak{S}_A$,

$$(\forall s \in S, \sigma s = s) \implies \sigma \cdot x = x$$

Remark: the set of supports of a element is closed by supset.

Definitions

(Cont'd)

Nominality

An element in a $\mathfrak{S}_A$-set admitting a finite support is said to be nominal.

A $\mathfrak{S}_A$-set X is nominal if every element of X is nominal.

Fact: the set of finite supports of a nominal element is closed under intersection.

Definitions

(Cont'd)

Nominality

An element in a $\mathfrak{S}_A$-set admitting a finite support is said to be nominal.

A $\mathfrak{S}_A$-set X is nominal if every element of X is nominal.

Fact: the set of finite supports of a nominal element is closed under intersection.

Support

Let x be a nominal element of a $\mathfrak{S}_A$-set. One defines *the* support of x by

$$\mathrm{supp}\,(x) = \bigcap\{\text{finite support of x}\}.$$

Remark: $\mathrm{supp}\,(x)$ is the smallest support of x.

Definitions

(Cont'd)

Nominality

An element in a $\mathfrak{S}_A$-set admitting a finite support is said to be nominal.

A $\mathfrak{S}_A$-set X is nominal if every element of X is nominal.

λ-terms example:
X is a nominal set because every term has a finite number of (free) variables

$$\text{supp}\,(t) = \mathrm{FV}(t)$$

Fact: the set of finite supports of a nom[...] intersection.

Support

Let x be a nominal element of a $\mathfrak{S}_A$-set. One defines *the* support of x by

$$\text{supp}\,(x) = \bigcap \{\text{finite support of x}\}.$$

Remark: $\text{supp}\,(x)$ is the smallest support of x.

Sheaf-rephrasing

Given X a nominal set, define

$$\begin{aligned} NX \colon \mathsf{Inj}_A &\to \mathsf{Set} \\ S &\mapsto \{x \in X : S \supseteq \operatorname{supp}(x)\} \end{aligned}$$

Sheaf-rephrasing

Given X a nominal set, define

$$\begin{aligned} NX \colon \mathsf{Inj}_A &\to \mathsf{Set} \\ S &\mapsto \{x \in X : S \supseteq \mathsf{supp}\,(x)\} \end{aligned}$$

But $\mathsf{Inj}_A \simeq \mathsf{Inj} \implies [\mathsf{Inj}_A, \mathsf{Set}] \simeq [\mathsf{Inj}, \mathsf{Set}]$, so one gets

$$N \colon \mathsf{Nom} \to [\mathsf{Inj}, \mathsf{Set}]\,.$$

Sheaf-rephrasing

Given X a nominal set, define

$$\begin{aligned} NX\colon \mathrm{Inj}_A &\to \mathrm{Set} \\ S &\mapsto \{x \in X : S \supseteq \mathrm{supp}\,(x)\} \end{aligned}$$

But $\mathrm{Inj}_A \simeq \mathrm{Inj} \implies [\mathrm{Inj}_A, \mathrm{Set}] \simeq [\mathrm{Inj}, \mathrm{Set}]$, so one gets

$$N\colon \mathrm{Nom} \to [\mathrm{Inj}, \mathrm{Set}]\,.$$

Theorem

N identifies Nom with those functors $\mathrm{Inj} \to \mathrm{Set}$ which preserve pullbacks.

Remark: It makes the nominal sets exactly the sheaves for a certain Grothendieck topology on Inj°. The topos of nominal sets is *Schanuel's topos*.

Sheaf-rephrasing

Given X a nominal set, define

$$\begin{aligned} NX \colon \mathsf{Inj}_A &\to \mathsf{Set} \\ S &\mapsto \{x \in X : S \supseteq \operatorname{supp}(x)\} \end{aligned}$$

But $\mathsf{Inj}_A \simeq \mathsf{Inj} \implies [\mathsf{Inj}_A, \mathsf{Set}] \simeq [\mathsf{Inj}, \mathsf{Set}]$, so one gets

$$N \colon \mathsf{Nom} \to [\mathsf{Inj}, \mathsf{Set}] \,.$$

λ-terms example:

View X as

$$\{x_j : j \in J \subset_f \mathbb{N}\} \mapsto \{\lambda\text{-terms with fv among the } x_j\text{'s}\}$$

Then pass to de Bruijn indices.

Theorem

N identifies Nom with

Remark: It makes the

Grothendieck topology on Inj°. The topos of nominal sets is *Schanuel's topos*.

2

Lawvere theories with arities

Classical algebraic theories

Classical algebraic theories

What is a monoid?

- a set M,
- a 2-ary multiplication $M^2 \to M$,
- a constant neutral $1 \to M$,

satisfying some axioms.

Classical algebraic theories

What is a monoid?

- a set M,
- a 2-ary multiplication $M^2 \to M$,
- a constant neutral $1 \to M$,

satisfying some axioms.

What is a group?

- a set G,
- a 2-ary multiplication $G^2 \to G$,
- a 1-ary inversion $G \to G$
- a constant neutral $1 \to G$,

satisfying some axioms.

Classical algebraic theories

What is a monoid?

- a set M,
- a 2-ary multiplication $M^2 \to M$,
- a constant neutral $1 \to M$,

satisfying some axioms.

What is a group?

- a set G,
- a 2-ary multiplication $G^2 \to G$,
- a 1-ary inversion $G \to G$
- a constant neutral $1 \to G$,

satisfying some axioms.

What is an algebraic structure?

- a set A,
- for each $n \geq 0$, a collection of n-ary operations $A^n \to A$

satisfying some axioms.

Categorical POV

What is an algebraic structure?

- a set A,
- for each $n \geq 0$, a collection of n-ary operations $A^n \to A$

satisfying some axioms.

Categorical POV

What is an algebraic structure?

- a set A,
- for each $n \geq 0$, a collection of n-ary operations $A^n \to A$

satisfying some axioms.

Denote $\aleph_0$ for the category of finite set $\mathbf{n} = \{0, \ldots, n-1\}$ and set-maps between them.

Lawvere theory

An algebraic structure is just a finite-product-preserving functor $A \colon \Theta^\circ \to \mathrm{Set}$ where

- there is a finite-sum-preserving bijective-on-objects functor $\aleph_0 \to \Theta$,
- morphisms $\mathbf{n} \to 1$ in Θ° are the n-ary operation.

The axioms are the commutative diagrams of Θ°.

Generalized algebraic structure by example

What is a category?

Generalized algebraic structure by example

What is a category?

- a graph C,
- for each $n \geq 0$, a "n-ary" composition map

$$\mathrm{Path}(n, C) \to C,$$

satisfying some axioms.

Generalized algebraic structure by example

What is a category?

- a graph C,
- for each $n \geq 0$, a "n-ary" composition map

$$\mathrm{Path}(n, C) \to C,$$

satisfying some axioms.

À la Lawvere

A category is just a functor $C\colon \Theta^\circ \to \mathsf{Set}$ where

- there is a "nice" functor $\boldsymbol{\Lambda} \to \Theta$, ($\boldsymbol{\Lambda}$ = finite linear graphs)
- morphisms $\Lambda_n \to \Lambda_1$ in Θ° are the compositions,

and such that $\exists G \in \mathsf{Graph},\ C(\Lambda_n) = \mathsf{Graph}\,(\Lambda_n, G)$.

The axioms are the commutative diagrams of Θ°.

Generalized algebraic structure

What is a generalized algebraic structure of arity $\mathbf{A} \hookrightarrow \mathbf{E}$?

Generalized algebraic structure

What is a generalized algebraic structure of arity $\mathbf{A} \hookrightarrow \mathbf{E}$?

- an object E in $\mathbf{E}$,
- for each $a, b \in \mathbf{A}$, a collection of "(a, b)-ary" operations

$$\mathbf{E}(a, E) \to \mathbf{E}(b, E),$$

satisfying some axioms.

Generalized algebraic structure

What is a generalized algebraic structure of arity $\mathbf{A} \hookrightarrow \mathbf{E}$?

- an object E in $\mathbf{E}$,
- for each $a, b \in \mathbf{A}$, a collection of "(a, b)-ary" operations

$$\mathbf{E}(a, E) \to \mathbf{E}(b, E),$$

satisfying some axioms.

(Berger, Melliès, Weber)

A generalized algebraic structure of arity $\mathbf{A} \hookrightarrow \mathbf{E}$ is just a functor $F \colon \Theta^\circ \to \mathrm{Set}$ where

- there is a "nice" functor $\mathbf{A} \to \Theta$,
- morphisms $a \to b$ in Θ° are the (a, b)-ary operations,

and such that $\exists E \in \mathbf{E},\ F(a) = \mathbf{E}(a, E)$.

The axioms are the commutative diagrams of Θ°.

Warnings!

Technicalities have been swept under the rug.

- The arity $\mathbf{A} \hookrightarrow \mathbf{E}$ can not be any embedding: there must exists $\mathbf{E} \hookrightarrow \mathrm{Psh}(\mathbf{A})$ such that the composite functor

$$\mathbf{A} \hookrightarrow \mathbf{E} \hookrightarrow \mathrm{Psh}(\mathbf{A})$$

  is the Yoneda embedding.
- The "niceness" of $j\colon \mathbf{A} \to \Theta$ is that the monad

$$j_* j_! \colon \mathrm{Psh}(\mathbf{A}) \to \mathrm{Psh}(\mathbf{A})$$

  should restict to a monad on $\mathbf{E}$.

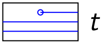
3

Quantum memory

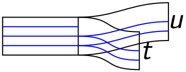
Quantum computation syntax

One construct ternary judgments: $\Delta \mid \Gamma \vdash t$.

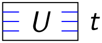
$$\frac{\Delta, a \mid \Gamma \vdash t}{\Delta \mid \Gamma \vdash \mathsf{new}(a.t)}$$



$$\frac{\Delta \mid \Gamma \vdash t \qquad \Delta \mid \Gamma \vdash u}{\Delta, a \mid \Gamma \vdash \mathsf{measure}(a, t, u)}$$



$$\frac{\Delta, \vec{b} \mid \Gamma \vdash t}{\Delta, \vec{a} \mid \Gamma \vdash \mathsf{apply}_U(\vec{a}, \vec{b}.t)} \qquad \forall U \in \mathbb{U}_{2^n}(\mathbb{C})$$



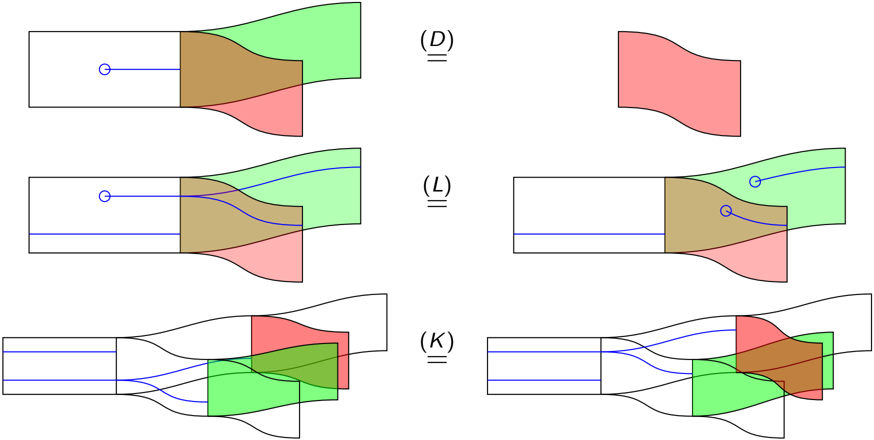
+ contraction/weakening rules on Γ (not Δ!) + permutations on both Δ et Γ.

Theory of quantum computation

There are 12 axioms. Just focus on those 3:

Theory of quantum computation

There are 12 axioms. Just focus on those 3:



Make it a generalized algebraic theory

Bij: the category of finite sets **n** and bijections.

Make it a generalized algebraic theory

Bij: the category of finite sets **n** and bijections.

$\Sigma \mathsf{Bij} \hookrightarrow \mathsf{Psh}(\mathsf{Bij})$: the full subcategory of finite sum of representable presheaves. So the objects of ΣBij are those finite sequence $(n_1, \ldots, n_k)$ of integers.

Make it a generalized algebraic theory

Bij: the category of finite sets **n** and bijections.

$\Sigma\mathrm{Bij} \hookrightarrow \mathrm{Psh}\,(\mathrm{Bij})$: the full subcategory of finite sum of representable presheaves. So the objects of ΣBij are those finite sequence $(n_1, \ldots, n_k)$ of integers.

Θ_Q: the category freely generated over ΣBij by

$$\begin{aligned} \mathsf{new} &\colon (0) \to (1) \\ \mathsf{measure} &\colon (1) \to (0, 0) \\ \mathsf{apply}_U &\colon (n) \to (n) \end{aligned}$$

and quotiented by the interpretations of the axioms.

Make it a generalized algebraic theory

Bij: the category of finite sets $\mathbf{n}$ and bijections.

$\Sigma\mathrm{Bij} \hookrightarrow \mathrm{Psh}(\mathrm{Bij})$: the full subcategory of finite sum of representable presheaves. So the objects of ΣBij are those finite sequence $(n_1, \ldots, n_k)$ of integers.

Θ_Q: the category freely generated over ΣBij by

$$\begin{aligned} \mathrm{new} &: (0) \to (1) \\ \mathrm{measure} &: (1) \to (0, 0) \\ \mathrm{apply}_U &: (n) \to (n) \end{aligned}$$

and quotiented by the interpretations of the axioms.

Why is it the theory of quantum computation?

Because $j_Q : \Sigma\mathrm{Bij} \to \Theta_Q$ is a generalized algebraic theory and its structures are exactly the models described in *Algebraic Effects, Linearity, and Quantum Programming Languages, by S.Staton*.

Back to nominal sets

By the same process, one can construct Θ_{coll} the category associated to the theory whose only operator is coll satisfying the axiom:

$$\mathsf{coll}(a, \mathsf{coll}(b, x)) = \mathsf{coll}(b, \mathsf{coll}(a, x)).$$

Back to nominal sets

By the same process, one can construct Θ_{coll} the category associated to the theory whose only operator is coll satisfying the axiom:

$$\mathrm{coll}(a, \mathrm{coll}(b, x)) = \mathrm{coll}(b, \mathrm{coll}(a, x)).$$

Fact

Θ_{coll} is isomorphic to $\Sigma(\mathrm{Inj}^{\circ})$. A generalized structure for $j_{\mathrm{coll}} : \Sigma\mathrm{Bij} \to \Theta_{\mathrm{coll}}$ is then identified with just a functor $\mathrm{Inj} \to \mathrm{Set}$.

Back to nominal sets

By the same process, one can construct Θ_{coll} the category associated to the theory whose only operator is coll satisfying the axiom:

$$\text{coll}(a, \text{coll}(b, x)) = \text{coll}(b, \text{coll}(a, x)).$$

Fact

Θ_{coll} is isomorphic to $\Sigma(\text{Inj}^\circ)$. A generalized structure for $j_{\text{coll}} : \Sigma\text{Bij} \to \Theta_{\text{coll}}$ is then identified with just a functor $\text{Inj} \to \text{Set}$.

Definition

A nominal set is a functor $\text{Inj} \to \text{Set}$ preserving pullbacks.

Back to nominal sets

By the same process, one can construct Θ_{coll} the category associated to the theory whose only operator is coll satisfying the axiom:

$$\mathsf{coll}(a, \mathsf{coll}(b, x)) = \mathsf{coll}(b, \mathsf{coll}(a, x)).$$

Fact

Θ_{coll} is isomorphic to $\Sigma(\mathsf{Inj}^{\circ})$. A generalized structure for $j_{\mathsf{coll}} : \Sigma\mathsf{Bij} \to \Theta_{\mathsf{coll}}$ is then identified with just a functor $\mathsf{Inj} \to \mathsf{Set}$.

Corollary

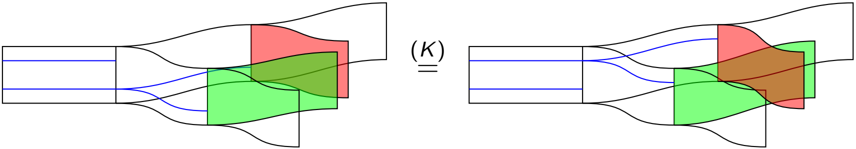
A nominal set is a model of j_{coll} sending the commutative diagrams

$$\begin{array}{ccc} n & \xrightarrow{\iota_i^n} & n+1 \\ {\scriptstyle \iota_{j-1}^n}\downarrow & & \downarrow{\scriptstyle \iota_j^{n+1}} \\ n+1 & \xrightarrow[\iota_i^{n+1}]{} & n+2 \end{array} \qquad (i < j)$$

to pullbacks.

Back to nominal sets

By the same process, one can construct Θ_{meas} the category associated to the theory whose only operator is meas satisfying the axiom:



Definition

A qnominal set is a model of j_{meas} sending the commutative diagrams

$$\begin{array}{ccccc}
(n,n,n,n) & \xleftarrow{(1\ 3\ 2\ 4)} & (n,n,n,n) & \xleftarrow{\mathrm{meas}_i^n \oplus \mathrm{meas}_i^n} & (n+1,n+1) \\
{\scriptstyle \mathrm{meas}_{j-1}^n \oplus \mathrm{meas}_{j-1}^n}\uparrow & & & & \uparrow{\scriptstyle \mathrm{meas}_j^{n+1}} \\
(n+1,n+1) & & \xleftarrow[\mathrm{meas}_i^{n+1}]{} & & n+2
\end{array}$$

to pullbacks.

Quantum support

With quantum nominality comes the notion of quantum support:

Support

For M a qnominal set, the quantum support of a element $x \in M_n$ is defined as

$$\operatorname{supp}(x) = \left\{ i \in \{0, \ldots, n-1\} : \forall y,\, x \neq \operatorname{meas}_i^{n-1}(y) \right\}.$$

Interpretation: the quantum support of a program is then the set of memory location for which the program is not a direct measure on it.

Quantum nominality is relevant

The theory Q contains meas and its axiom, so it makes sense to ask whether a model of Q is qnominal or not.

Proposition

Any model of Q is a qnominal set.

Quantum nominality is relevant

The theory Q contains meas and its axiom, so it makes sense to ask whether a model of Q is qnominal or not.

Proposition

Any model of Q is a qnominal set.

Preuve.

All is left to show is that if $x \in M_2$ can be written

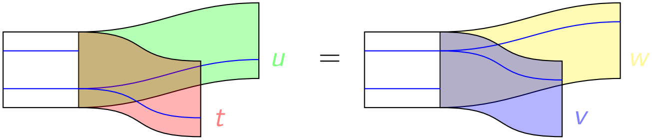
$$\text{measure}(a, t, u) = x = \text{measure}(b, v, w),$$

then $\exists y_1, y_2, y_3, y_4 \in M_0$,

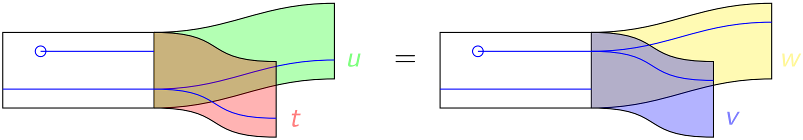
$$t = \text{measure}(b, y_1, y_2), \quad u = \text{measure}(b, y_3, y_4)$$
$$v = \text{measure}(a, y_1, y_3), \quad w = \text{measure}(a, y_2, y_4)$$

□

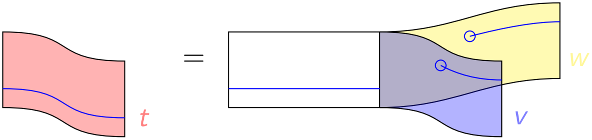
Draw the proof!



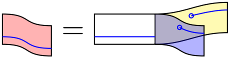
Draw the proof!



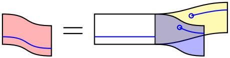
Draw the proof!

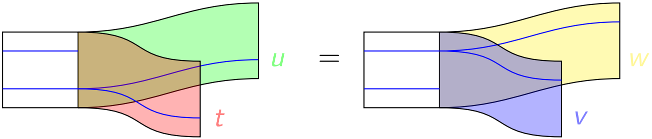


Draw the proof!

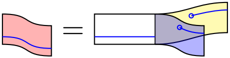


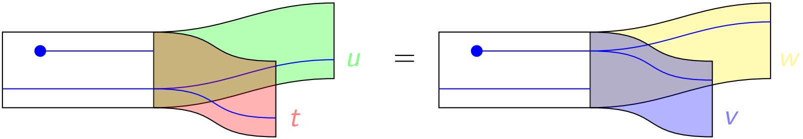
Draw the proof!



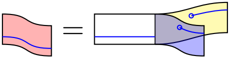


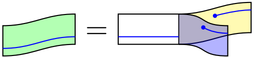
Draw the proof!

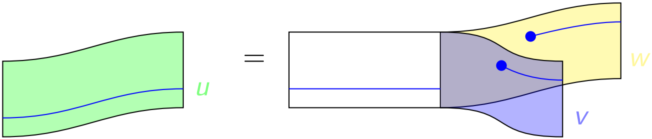




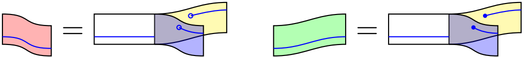
Draw the proof!

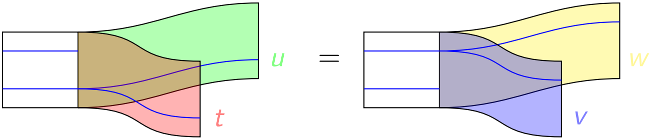




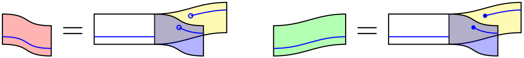


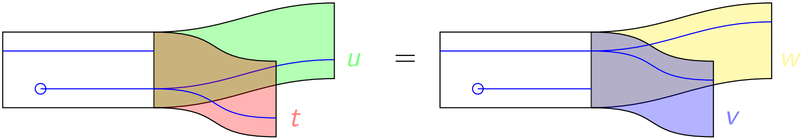
Draw the proof!



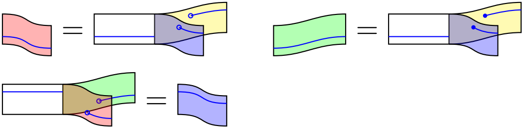


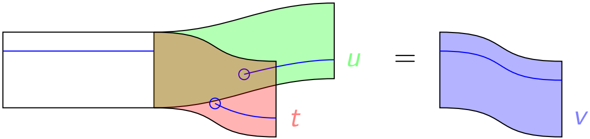
Draw the proof!



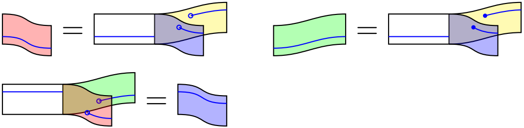


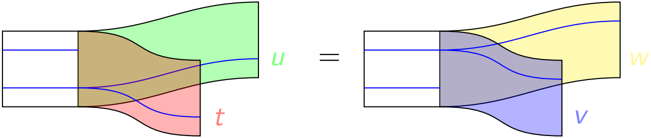
Draw the proof!



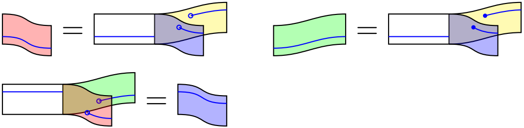


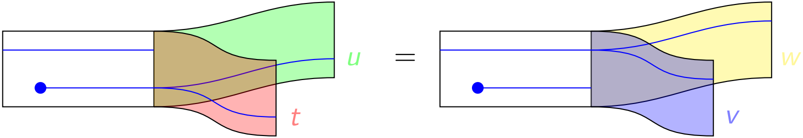
Draw the proof!



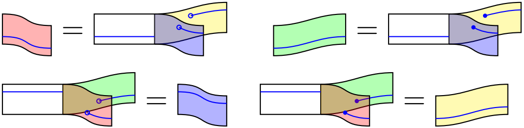


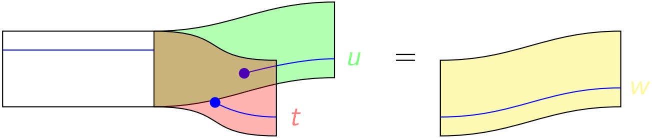
Draw the proof!



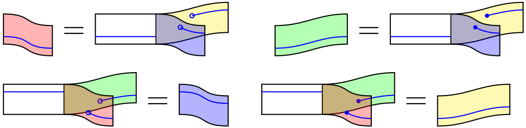


Draw the proof!

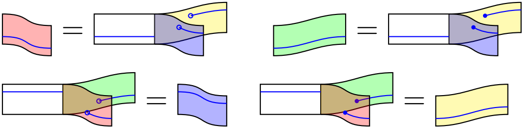


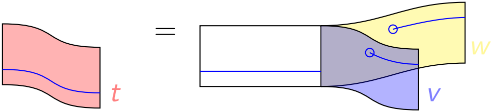


Draw the proof!

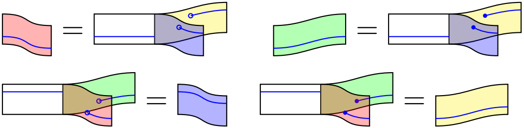


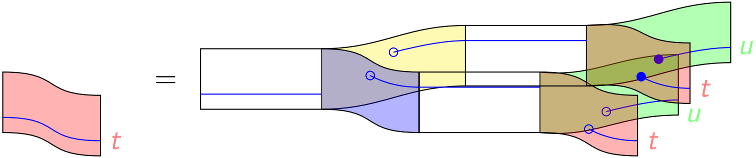
Draw the proof!



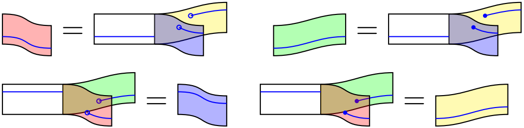


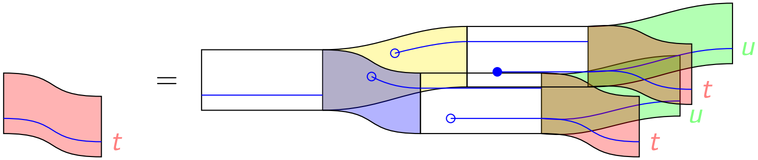
Draw the proof!



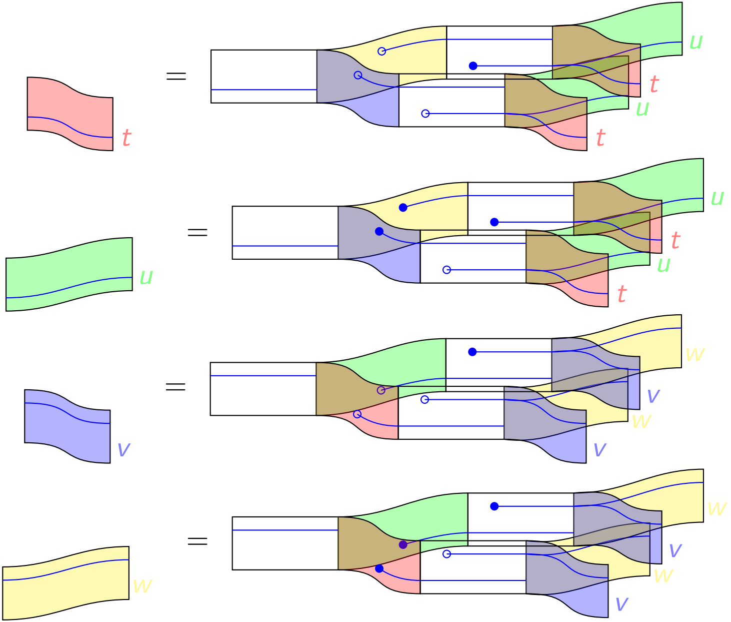


Draw the proof!





Draw the proof!



Thanks.

If interested, one can find a complete internship report on my webpage:
`http://www.eleves.ens.fr/home/cagne/`