From profinite words to profinite λ-terms

Vincent Moreau, joint work with Paul-André Melliès and Sam van Gool

LHC days, ENS Paris-Saclay

October 12, 2022

IRIF, Université Paris Cité, Inria Paris

Context of the talk

Two different kinds of automata:

- Deterministic automata (in **FinSet**)
- Non-deterministic automata (in **FinRel**)

Profinite methods are well established for words using finite monoids.

Contribution: definition of profinite λ-terms in any model and proof that

Profinite words are in bijection with deterministic profinite λ-terms

using the Church encoding of words and Reynolds parametricity.

This leads to a notion of non-deterministic profinite λ-term in **FinRel**.

Interpreting words as λ-terms

Simply typed λ-terms

λ-terms are defined by the grammar

$$M, N \quad ::= \quad x \mid \lambda x.M \mid MN.$$

Simple types are generated by the grammar

$$A, B \quad ::= \quad o \mid A \Rightarrow B.$$

For simple types, typing derivations are generated by the following three rules:

$$\frac{}{\Gamma, x : A \vdash x : A}\ \texttt{Var} \qquad \frac{\Gamma \vdash M : A \Rightarrow B \qquad \Gamma \vdash N : A}{\Gamma \vdash MN : B}\ \texttt{App} \qquad \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x.M : A \Rightarrow B}\ \texttt{Abs}$$

The Church encoding for words

Any natural number n can be encoded in the simply typed λ-calculus as

$$s : o \Rightarrow o,\ z : o \vdash \underbrace{s\,(\ldots(s\,z))}_{n \text{ applications}} : o.$$

A natural number is just a word over a one-letter alphabet.

For example, the word *abba* over the two-letter alphabet $\{a, b\}$

$$a : o \Rightarrow o,\ b : o \Rightarrow o,\ c : o \vdash a\,(b\,(b\,(a\,c))) : o.$$

is encoded as the closed λ-term

$$\lambda a.\lambda b.\lambda c.a\,(b\,(b\,(a\,c)))\ :\ \underbrace{(o \Rightarrow o)}_{\text{letter } a} \Rightarrow \underbrace{(o \Rightarrow o)}_{\text{letter } b} \Rightarrow \underbrace{o}_{\text{input}} \Rightarrow \underbrace{o}_{\text{output}}.$$

Categorical interpretation

Let **C** be a cartesian closed category.

In order to interpret the simply typed λ-calculus in **C**, we pick an object Q of **C** in order to interpret the base type o and define, for any simple type A, the object

$$[\![A]\!]_Q$$

by induction, as follows:

$$\begin{array}{rcl} [\![\mathrm{o}]\!]_Q & := & Q \\ [\![A \Rightarrow B]\!]_Q & := & [\![A]\!]_Q \Rightarrow [\![B]\!]_Q. \end{array}$$

The simply typed λ-terms are then interpreted by structural induction on their type derivation using the cartesian closed structure of **C**.

The category FinSet

Fact. The category **FinSet** is cartesian closed: there is a bijection

$$\mathbf{FinSet}(A \times B, C) \quad \cong \quad \mathbf{FinSet}(B, A \Rightarrow C)$$

natural in A and C, where $A \Rightarrow C$ is the set of functions from A to C.

In particular, given a finite set Q used to interpret ϕ, every word w over the alphabet $\Sigma = \{a, b\}$ seen as a λ-term

$$\vdash w \ : \ \underbrace{(\phi \Rightarrow \phi)}_{\text{letter } a} \Rightarrow \underbrace{(\phi \Rightarrow \phi)}_{\text{letter } b} \Rightarrow \underbrace{\phi}_{\text{input}} \Rightarrow \underbrace{\phi}_{\text{output}}$$

can be interpreted in **FinSet** as

$$[\![w]\!]_Q \quad \in \quad (Q \Rightarrow Q) \Rightarrow (Q \Rightarrow Q) \Rightarrow Q \Rightarrow Q$$

which describes how the word will interact with a deterministic automaton.

Entering the profinite world

Profinite words

Definition. A **profinite word** is a family of maps

$$u_M \quad : \quad [\Sigma, M] \longrightarrow M \qquad \text{where } M \text{ ranges over all finite monoids}$$

such that for every function $p : \Sigma \to M$ and homomorphism $\varphi : M \to N$, with M and N finite monoids, we have $u_N(\varphi \circ p) = \varphi(u_M(p))$, i.e. the following diagram commutes:

$$\begin{tikzcd}
{[\Sigma, M]} \arrow[r, "\varphi\circ -"] \arrow[d, "u_M"'] & {[\Sigma, N]} \arrow[d, "u_N"] \\
M \arrow[r, "\varphi"'] & N
\end{tikzcd} .$$

Remark. Any word $w = a_1 \dots a_n$ induces a profinite word u whose components are

$$u_M \quad : \quad p \longmapsto p(a_1) \dots p(a_n) \qquad \text{where } M \text{ ranges over all finite monoids.}$$

A profinite word which is not a word

In any finite monoid M, all elements $m \in M$ have a unique power m^n (for $n \geq 1$) which is idempotent, i.e. such that $m^n m^n = m^n$. It is obtained for $n = |M|!$.

Let a be any letter in Σ. The family of maps

$$u_M \quad : \quad \begin{array}{ccc} [\Sigma, M] & \longrightarrow & M \\ p & \longmapsto & p(a)^{|M|!} \end{array} \qquad \text{where } M \text{ ranges over all finite monoids}$$

is an profinite word written a^ω which is not a finite word.

The set of profinite words is endowed with a monoid structure computed pointwise. In that setting, a^ω is idempotent.

Key property: parametricity of profinite words

Definition. Given M, N two finite monoids and $R \subseteq M \times N$, we say that R is a **monoidal relation** $M \nrightarrow N$ if it is a submonoid of $M \times N$. This means that

$$(e_M, e_N) \in R \qquad \text{and} \qquad \text{for all } (m,n) \text{ and } (m',n') \text{ in } R, \text{ we have } (mm', nn') \in R.$$

Proposition. Let $u = (u_M)$ be a family of maps. The following are equivalent:

- u is profinite
- for every pair of functions $p : \Sigma \to M$ and $q : \Sigma \to N$ with M and N finite monoids, and for any monoidal relation $R : M \nrightarrow N$,

$$\text{if for all } a \in \Sigma \text{ we have } (p(a), q(a)) \in R, \qquad \text{then } (u_M(p), u_N(q)) \in R.$$

Parametric λ-terms

Definition of logical relations

Recall that for any set Q we have defined the set

$$[\![A]\!]_Q$$

by structural induction on the type A.

We extend the construction to set-theoretic relations $R : P \nrightarrow Q$, giving a relation

$$[\![A]\!]_R \quad : \quad [\![A]\!]_P \nrightarrow [\![A]\!]_Q \ .$$

by structural induction on the type A:

$$\begin{aligned}
[\![o]\!]_R \quad &:= \quad R \\
[\![A \Rightarrow B]\!]_R \quad &:= \quad \{\ (f, g) \in [\![A \Rightarrow B]\!]_P \times [\![A \Rightarrow B]\!]_Q \mid \\
&\qquad\qquad \text{for all } x \in [\![A]\!]_P \text{ and } y \in [\![A]\!]_Q \ , \\
&\qquad\qquad\qquad \text{if } (x, y) \in [\![A]\!]_R \text{ then } (f(x), g(y)) \in [\![B]\!]_R \ \}.
\end{aligned}$$

Double categories and main example

A double category is given by the data of objects together with

- 1-cells: vertical ($\rightarrow$) and horizontal ($\nrightarrow$) arrows,
- 2-cells: squares ($\Rightarrow$) between pairs of vertical and horizontal arrows which can be composed both horizontally or vertically.

Example. the category whose objects are finite sets, vertical arrows are functions, horizontal arrows are relations and whose squares are unique and exist when:

$$\begin{tikzcd} X \arrow[r, "R", "|" marking] \arrow[d, "f"'] \arrow[dr, phantom, "\Downarrow"] & Y \arrow[d, "g"] \\ X' \arrow[r, "R'"', "|" marking] & Y' \end{tikzcd} \quad \text{iff} \quad \forall x \in X, y \in Y, \quad \text{if } (x, y) \in R \quad \text{then } (f(x), g(y)) \in R'$$

The category **Cat** of categories has pullbacks.

Definition. A double category is a diagram

$$\begin{tikzcd} D_1 \arrow[d, bend right, "s"'] \arrow[d, bend left, "t"] \\ D_0 \arrow[u, "i"'] \end{tikzcd}$$

where $s \circ i = \mathbf{Id}_{D_0} = t \circ i$, together with $m : D_1 \times_{D_0} D_1 \to D_1$ such that $s \circ m = s \circ \pi_1$ and $t \circ m = t \circ \pi_2$ such that the following monoidal identities hold:

$$\begin{tikzcd} D_1 \times_{D_0} D_1 \times_{D_0} D_1 \arrow[r, "\mathbf{Id}_{D_1} \times m"] \arrow[d, "m \times \mathbf{Id}_{D_1}"'] & D_1 \times_{D_0} D_1 \arrow[d, "m"] \\ D_1 \times_{D_0} D_1 \arrow[r, "m"'] & D_1 \end{tikzcd}
\qquad
\begin{tikzcd} D_1 \times_{D_0} D_0 \arrow[r, "\mathbf{Id}_{D_1} \times i"] \arrow[dr, "\pi_1"'] & D_1 \times_{D_0} D_1 \arrow[d, "m"] & D_0 \times_{D_0} D_1 \arrow[l, "i \times \mathbf{Id}_{D_1}"'] \arrow[dl, "\pi_2"] \\ & D_1 & \end{tikzcd}$$

FinSet as an internal category

Example. We can endow **FinSet** with a structure of double category:

- the category D_0 is **FinSet**
- the category D_1 is the category whose objects are relations $R : X \nrightarrow Y$ and a morphism $f : (R : X \nrightarrow Y) \to (R' : X' \nrightarrow Y')$ is a pair of functions $f_1 : X \to X'$ and $f_2 : Y \to Y'$ such that

$$\text{if} \quad (x, y) \in R \quad \text{then} \quad (f_1(x), f_2(y)) \in R' \ .$$

We take $s(R : X \nrightarrow Y) = X$ and $t(R : X \nrightarrow Y) = Y$. If $R : X \nrightarrow Y$ and $R' : Y \nrightarrow Z$, we let

$$m(R, R') = R \circ R' = \{(x, z) \in X \times Z \mid \exists y \in Y, (x, y) \in R, (y, z) \in R'\} \ .$$

Cartesian double categories

A double category $\mathbf{D}$ is cartesian if the pairs of squares

$$\begin{tikzcd} X \arrow[r, "R", "\shortmid"{marking}] \arrow[d, "f_1"'] \arrow[dr, phantom, "\Downarrow C_1"] & Y \arrow[d, "g_1"] \\ X_1 \arrow[r, "S_1"', "\shortmid"{marking}] & Y_1 \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, "R", "\shortmid"{marking}] \arrow[d, "f_2"'] \arrow[dr, phantom, "\Downarrow C_2"] & Y \arrow[d, "g_2"] \\ X_2 \arrow[r, "S_2"', "\shortmid"{marking}] & Y_2 \end{tikzcd}$$

is in bijection with the set of squares

$$\begin{tikzcd} X \arrow[r, "R", "\shortmid"{marking}] \arrow[d, "\langle f_1, f_2 \rangle"'] \arrow[dr, phantom, "\Downarrow \langle C_1, C_2 \rangle"] & Y \arrow[d, "\langle g_1, g_2 \rangle"] \\ X_1 \times X_2 \arrow[r, "S_1 \times S_2"', "\shortmid"{marking}] & Y_1 \times Y_2 \end{tikzcd}$$

and the horizontal morphism $\mathbf{Id}_1 : 1 \nrightarrow 1$ is terminal.

Internally: D_0 and D_1 are cartesian and s and t strictly respect the cartesian structure.

Cartesian closed double categories

A cartesian double category **D** is closed if the set of squares

$$\begin{tikzcd} X_1 \times X_2 \arrow[r, "R_1 \times R_2", "\shortmid"{marking}] \arrow[d, "f"'] \arrow[dr, phantom, "\Downarrow C"] & Y_1 \times Y_2 \arrow[d, "g"] \\ X \arrow[r, "R"', "\shortmid"{marking}] & Y \end{tikzcd}$$

is in bijection with the set of squares

$$\begin{tikzcd} X_2 \arrow[r, "R_2", "\shortmid"{marking}] \arrow[d, "\mathrm{Cur}(f)"'] \arrow[dr, phantom, "\Downarrow \mathrm{Cur}(C)"] & Y_2 \arrow[d, "\mathrm{Cur}(g)"] \\ X_1 \Rightarrow X \arrow[r, "R_1 \Rightarrow R"', "\shortmid"{marking}] & Y_1 \Rightarrow Y \end{tikzcd}$$

Internally: D_0 and D_1 are CCCs and s and t strictly respect the CCC structure.

Fact. The double category of finite sets is cartesian closed.

Parametric λ-terms

Let us consider a cartesian closed double category.

Definition. Let A be a simple type. A **parametric λ-term** of type A is the data

- a family of vertical maps $\theta_Q : 1 \to [\![A]\!]_Q$ where Q ranges over all objects
- a family of squares $\theta_R : \mathbf{Id}_1 \Rightarrow [\![A]\!]_R$ where R ranges over all horizontal arrows

such that the horizontal source and target of a square θ_R for $R : P \nrightarrow Q$ are the maps θ_P and θ_Q, which we can represent as

$$\begin{tikzcd} 1 \arrow[r, "\mathbf{Id}_1", "\shortmid"{marking}] \arrow[d, "\theta_P"'] \arrow[dr, phantom, "\Downarrow \theta_R"] & 1 \arrow[d, "\theta_Q"] \\ {[\![A]\!]_P} \arrow[r, "{[\![A]\!]_R}"', "\shortmid"{marking}] & {[\![A]\!]_Q} \end{tikzcd}$$

Parametric λ-terms and profinite words

In the case of **FinSet**, a parametric λ-term of type A amounts to a family

$$\theta_Q \quad \in \quad [\![A]\!]_Q \qquad \text{where } Q \text{ ranges over all finite sets,}$$

such that, for every binary relation $R \colon P \nrightarrow Q$, we have

$$(\theta_P, \theta_Q) \quad \in \quad [\![A]\!]_R \; .$$

Theorem. Parametric λ-terms define a cartesian closed category, and the parametric λ-terms of type

$$\mathbf{Church}_\Sigma \quad := \quad \underbrace{(\mathtt{o} \Rightarrow \mathtt{o}) \Rightarrow \ldots \Rightarrow (\mathtt{o} \Rightarrow \mathtt{o})}_{|\Sigma| \text{ times}} \Rightarrow (\mathtt{o} \Rightarrow \mathtt{o})$$

are in bijection with the profinite words on Σ.

Conclusion

Current & future work:

- investigate the metric side of the profinite words in the setting of λ-terms;
- determine the parametric λ-terms of type Church_Σ in the model associated to nondeterministic automata;
- investigate a generalization of logic on words with MSO to a logic on λ-terms.

Conclusion

Current & future work:

- investigate the metric side of the profinite words in the setting of λ-terms;
- determine the parametric λ-terms of type Church_Σ in the model associated to nondeterministic automata;
- investigate a generalization of logic on words with MSO to a logic on λ-terms.

Thank you for your attention!

Any questions?

Bibliography

[Geh13] Mai Gehrke. *Stone duality, topological algebra, and recognition*. 2013. DOI: `10.48550/ARXIV.1309.2422`. URL: `https://arxiv.org/abs/1309.2422`.

[GS16] Samuel J. v. Gool and Benjamin Steinberg. *Pro-aperiodic monoids via saturated models*. 2016. DOI: `10.48550/ARXIV.1609.07736`. URL: `https://arxiv.org/abs/1609.07736`.

[Mel17] Paul-André Melliès. "Higher-order parity automata". In: *Proceedings of the 32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, 2017*. 2017, pp. 1–12.

[Pin] Jean-Eric Pin. "Profinite Methods in Automata Theory". In: *26th International Symposium on Theoretical Aspects of Computer Science STACS 2009*. IBFI Schloss Dagstuhl. URL: `https://hal.inria.fr/inria-00359677`.

The inverse bijections T and W

Pro $\to$ Para. Every profinite word u induces a parafinite term with components

$$T(u)_Q \quad : \quad \begin{array}{ccc} \Sigma \Rrightarrow (Q \Rrightarrow Q) & \longrightarrow & Q \Rrightarrow Q \\ p & \longmapsto & u_{Q \Rrightarrow Q}(p) \end{array}$$

given the fact that $Q \Rrightarrow Q$ is a monoid for the function composition.

Para $\to$ Pro. Every parametric term θ induces a profinite word with components

$$W(\theta)_M \quad : \quad \begin{array}{ccc} \Sigma \Rrightarrow M & \longrightarrow & M \\ p & \longmapsto & \theta_M(i_M \circ p)(e_M) \end{array}$$

$$\begin{tikzcd} \Sigma \Rrightarrow (M \Rrightarrow M) \arrow[r, "\theta_M"] & M \Rrightarrow M \arrow[d, "-(e_M)"] \\ \Sigma \Rrightarrow M \arrow[u, "i_M \circ -"] \arrow[r, dashed, "W(\theta)_M"'] & M \end{tikzcd}$$

where $i_M : M \to (M \Rrightarrow M)$ is the Cayley embedding.

These are bijections between profinite words and parametric λ-terms.

Let u be a profinite word. Recall that $u_M : (\Sigma \Rightarrow M) \to M$.

Its associated parametric λ-term $T(u)$ has components

$$T(u)_Q = u_{(Q \Rightarrow Q)}$$

Its associated profinite word $W(T(u))$, for $p : \Sigma \to M$, is equal to

$$W(T(u))_M(p) = T(u)_M(i_M \circ p)(e_M) = u_{(M \Rightarrow M)}(i_M \circ p)(e_M)$$

In order to show that $W(T(u))$ is u, we use the parametricity of profinite words.

We consider the moinoidal logical relation $R \subseteq (M \Rightarrow M) \times M$ defined as

$$R \quad := \quad \{(f, m) \in (M \Rightarrow M) \times M \mid \forall n \in M,\ f(n) = m \cdot n\}$$

We have that $(i_M \circ p, p) \in [\![\mathbb{O} \times \cdots \times \mathbb{O}]\!]_R$ because for all $a \in \Sigma$,

$$\text{for all } m \in I, \qquad (i_M \circ p)(a)(m) = p(a) \cdot m.$$

By parametricity of u applied to R, we have that

$$(u_{(M \Rightarrow M)}(i_M \circ p), u_M(p)) \quad \in \quad [\![\mathbb{O} \Rightarrow \mathbb{O}]\!]_R$$

which means, by definition of $[\![\mathbb{O} \Rightarrow \mathbb{O}]\!]_R$, that

$$\text{for all } (f, m) \in R, \quad \text{we have } (u_{(M \Rightarrow M)}(i_M \circ p)(f), u_M(p)(m)) \in R$$

which gives the desired result:

$$W(T(u)) = u_{(M \Rightarrow M)}(i_M \circ p)(e_M) = u_M(p)(m).$$

Let θ be a parafinite term. Recall that $\theta_Q \in (\Sigma \Rightarrow (Q \Rightarrow Q)) \Rightarrow (Q \Rightarrow Q)$.

Its associated profinite word $W(\theta)$ is equal, for $p : \Sigma \to M$, to

$$W(\theta)_M(p) = \theta_M(i_M \circ p)(e_M).$$

Its reassociated parametric λ-term $T(W(\theta))$ has components

$$T(W(\theta))_Q = W_{(Q \Rightarrow Q)}.$$

We want to show that, for all $p : \Sigma \to (Q \Rightarrow Q)$, we have $\theta_Q(p) = T(W(\theta))_Q(p)$, i.e.

$$\text{for all } q_0 \in Q, \qquad \theta_{(Q\Rightarrow Q)}(i_{(Q\Rightarrow Q)} \circ p)(\mathbf{Id}_Q)(q_0) = \theta_Q(p)(q_0)$$

To show that, we introduce, for any $q_0 \in Q$, the logical relation

$$R_{q_0} \quad := \quad \{(f, q) \in (Q \Rightarrow Q) \times Q \mid f(q_0) = q\}.$$

First, we have $(i_{(Q \Rightarrow Q)} \circ p, p) \in [\![(\Phi \Rightarrow \Phi) \times \cdots \times (\Phi \Rightarrow \Phi)]\!]_{R_{q_0}}$ because for all $a \in \Sigma$,

$$\text{for all } (f, q) \in R, \quad \text{we have } (i_{(Q \Rightarrow Q)} \circ p)(a)(f)(q_0) = p(a)(f(q_0)) = p(a)(q)$$

By parametricity of θ, we obtain that $(\theta_{(Q \Rightarrow Q)}(i_{(Q \Rightarrow Q)} \circ p), \theta_Q(p)) \in [\![\Phi \Rightarrow \Phi]\!]_{R_{q_0}}$.
Given the fact that $(\mathsf{Id}_Q, q_0) \in R_{q_0}$ and by definition of $[\![\Phi \Rightarrow \Phi]\!]_{R_{q_0}}$, we obtain that

$$\theta_{(Q \Rightarrow Q)}(i_{(Q \Rightarrow Q)} \circ p)(\mathsf{Id}_Q)(q_0) = \theta_Q(p)(q_0)$$

which concludes the proof. $\square$