# New results on the Non-Structural Subtype Entailment Problem

Flavien BREUVART, Vincent PENELLE, Jakob REHOF

November 7th 2019

# Naive polymorphism

## We fix a set of monomorphic types

We only consider $\mathbb{T}_\mu$ and $\mathbb{T}_\nu$ that are the the inductives and coinductives fixpoints over the grammar

$$s, t := \quad \bot \quad | \quad \top \quad | \quad s \times t \quad | \quad s \to t$$

## Polymorphic type

A polymorphic type $\mathbb{P}$ is an inductive type over the grammar :

$$s, t := \quad u \quad | \quad \bot \quad | \quad \top \quad | \quad s \times t \quad | \quad s \to t$$

for $u, v..$ over a set of types variables.

## Order on polymorphic types

A sequent $s \leq t$ is true iff for all instanciations $\rho : \mathbb{P} \to \mathbb{T}$, $s\rho \leq t\rho$.

Remark : different orders for $\mathbb{T}_\mu$ and $\mathbb{T}_\nu$, we consider $\mathbb{T}_\nu$ that is slightly easier to deal with

# A non extensible notion of type judgement

**You can't use new types operators**

We have :

$$(\bot \to \top) \to \bot \quad \leq \quad (u \to \bot) \vee u$$

Either $u = \top$ or a product and $(u \to \bot) \vee u = \top$,
or $u$ is a function and $\bot \to \top \geq u$ as $\bot \to \top$ is above all functions.

This is not true anymore if we add a type that is not between $\bot \to \top$ and $\top$ such as a types for effectful functions.

# Why am I interested in the subject

## Resources are preexisting

The algebras of resources we are trying to approximate are fixed.

We want to be able to use every available arguments to specify them.

## Resources never structural

Our order represent our knowledge on the used resource...

However, unresourced types should be vanilla ML.

The real reason : Jakob challenged me :p

The real real reason : I needed to understand subtilties of subtype entailment

# The NSSE problem (TLCA LOOP 16)

In order to apply type inference, one not only have to decide the order relation, but have to decide it over a context.

## The Non-Structural subtype Entailment (NSSE) problem

Given a set of polymorphic inequation $\psi = (t_1 \leq s_1, ...., t_n \leq s_n)$, and a specific inequation $t \leq s$, do we have :

$$\forall \rho, \quad \rho \Vdash (t_1 \leq s_1 \text{ and } \cdots \text{ and } t_n \leq s_n) \Rightarrow t \leq s$$

we use for notation $\psi \vdash t \leq s$

**Theorem [Henglein&Rehof98]**
NSSE is PSpace hard

**Open [Pottier 1996]**
Is NSSE decidable ?

# Restricting to the product and simple equations

## simple equations

Simple equations are of the form $x \leq y$, $x \odot y \leq z$ or $x \leq y \odot z$ for $x, y, z$ variables or $\bot$ or $\top$ and for $\odot$ either $\times$ or $\to$.

## Equations cans always be reformulated

$\vdash (\bot \to \top) \to \bot \leq (v \to \bot) \vee v$ can be reformulated as

$$x \leq u \to \bot, \quad \bot \to \top \leq u, \quad v \leq y, \quad v \to \bot \leq y \quad \vdash x \leq y$$

for free

## In fact the product restriction is already complex

$$x \leq y \times \bot, \quad z \times y \leq y, \quad z \times \top \leq z \quad \vdash \quad x \leq y$$

real restriction

## From now on : only product and simple equations

We also require $x \leq y$ as conclusion and no $u \leq v$ as hypothesis.

# The NSSE(×) problem

**Theorem [Niehren&Priesnitz03] : NSSE(×) is PSpace hard**

**Theorem [N&P03] : A PSpace restriction**

restrict $\phi \in \texttt{Constr}(\times)$ with no appearance of $\bot$ or $\top$

**Our result : A 2-ExpTime restriction**

restrict $\phi \in \texttt{Constr}(\times)$ with no appearance of $\bot \times \bot$ or $\top \times \top$.

Alternatively, our proof also work if we consider a type system that equates $\top = \top \times \top$ and $\bot = \bot \times \bot$.

# Priesnitz's thesis : translation to cap languages

## Capping operation on languages

$$R^o := \{u \in \mathtt{prefix}(v^\omega) \mid v \in R\}$$

## Priesnitz' reduction

NSSE($\times$) reduces to the

$$\text{Universality of } \sum_i R_i S_i^o$$

for $(R_i, S_i)_i$ rational

## More precisely

The two following are equireducible :

- Universality of $\sum_i (R_i S_i^o + R_i^{\leq}) + K$
  given $(R_i, S_i)_i$ rationals and $K$ rational and suffix-close.
- $\phi \vdash x \leq y$ given $\phi$

# Niehren and Priesnitz' idea in 5 steps

## Step 1 : Decomposing into two symmetric properties

$\phi \vdash x \leq y$ iff for all $\rho$ satisfying $\phi$, and all path $\pi \in \{1,2\}^*$,

1. if there is a $\top$ along $\rho(x).\pi$, there is one along $\rho(y).\pi$,
2. if there is a $\bot$ along $\rho(y).\pi$, there is one along $\rho(x).\pi$.

## Step 2 : Constructibility + double negation

the condition (1.) is true iff for all path $\pi \in \{1,2\}^*$ :

1*a*. when there is no proof (using $\psi$) that $y.\pi$ can reach a $\top$,

12. then there is no proof (using $\psi$) that $x.\pi$ can reach a $\top$.

## Step 3 : Safety and reachability conditions

the condition (1.) is true if for all path $\pi \in \{1,2\}^*$ :

1*a*. either $\top$ is always reached from $y$ following $\pi$.

1*b*. or $\pi$ is safe from having a $\top$ starting from from $x$,

1$b'$. or $x.\pi$ and $y.\pi$ can be shown equal

# Niehren and Priesnitz' idea in 5 steps

## Step 4 : an additional safety condition

the condition (1.) is true iff for all path $\pi \in \{1,2\}^*$ :

1*a*. either $\top$ is always reached from $y$ following $\pi$.

1*b*. or $\pi$ is safe from having a $\top$ starting from from $x$,

1$b'$. or $x.\pi$ and $y.\pi$ reach a point where they are equal,

1$b''$. or starting from some point $x.\pi$ visit the same path as $y.\pi$ with some delay.

## Step 5 : Build your cap-automata out of it

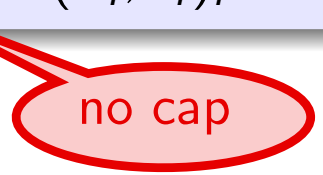
Example on $x \leq y \times \bot,\ z \times y \leq y,\ z \times \top \leq z \vdash x \leq y$

# Decidable Variants

## [Niehren& Priesnitz' 99]

The two following are equivalent :

- $\phi \vdash x \leq y$ for any $\phi$ with no appearance of $\bot$ or $\top$.
- universality of $\sum_i (R_i S_i)^{\leq}$ for $(R_i, S_i)_i$ rationals,




## The variant that we use

- $\phi \vdash x \leq y$ for any $\phi$ with no appearance of $\bot \times \bot$ or $\top \times \top$,
- universality of $\sum_i (R_i S_i^o + R_i^{\leq}) + K$ for $(R_i, S_i)_i$ rationals and $K$ rational, suffix-close and saturated in the sense that $\omega \in K$ whenever $\omega a \in K$ for every $a$.

# Idea : looking at the infinity

## Büchi completion

$$\overline{L} := \{\mu \in \Sigma^\omega \mid u \in L \text{ for infinitely many } u \preceq \mu\}$$

## Fundamental property

$$\overline{RS^o} = \overline{RS} + \sum_{u \in S} Ru^\omega$$

## Idea

$\overline{RS}$ has wide holes

$\sum_{u \in S} Ru^\omega$ is very sparse

# Idea : looking at the infinity

## Idea

$\overline{RS}$ has wide holes

$\sum_{u \in S} Ru^\omega$ is very sparse

## Can be formalised into

There is (constructively) a finite set $F \subseteq S$, such that $\overline{RS^o}$ is universal iff $\overline{RS} + \sum_{u \in F} Ru^\omega$ is universal.

## Can be extended to

There is (constructively) finite sets $(F_i \subseteq S_i)$, such that $\overline{\sum_i (R_i S_i^o) + K}$ is universal iff $\overline{\sum_i RS_i + K} + \sum_i \sum_{u \in F_i} R_i u^\omega$ is universal.

University of Büchi automaton is PSpace

# Idea : looking at the infinity

## Idea

$\overline{RS}$ has wide holes

$\sum_{u \in S} Ru^\omega$ is very sparse

## Can be formalised into

There is (constructively) a finite set $F \subseteq S$, such that $\overline{RS^o}$ is universal iff $\overline{RS} + \sum_{u \in F} Ru^\omega$ is universal.

## Can be extended to

There is (constructively) finite sets $(F_i \subseteq S_i)$, such that $\overline{\sum_i (R_i S_i^o) + K}$ is universal iff $\overline{\sum_i RS_i + K} + \sum_i \sum_{u \in F_i} R_i u^\omega$ is universal.

University of Büchi automaton is PSpace

white lie

# The issue : how to come back ?

$$\sum_i (R_i S_i^o + R_i^{\leq}) + K \text{ universal}$$

$$\Rightarrow \quad \overline{\sum_i (R_i S_i^o + R_i^{\leq}) + K} \text{ universal}$$

$$\text{iff} \quad \overline{\sum_i (R_i S_i^o + R_i^{\leq})} + \overline{K} \text{ universal}$$

$$\text{iff} \quad \overline{K}^c \subseteq \overline{\sum_i (R_i S_i^o + R_i^{\leq})}$$

$$\text{iff} \quad \mathtt{pref}(\overline{K}^c) \subseteq \mathtt{pref}(\overline{\sum_i (R_i S_i^o + R_i^{\leq})})$$

$$\Rightarrow \quad \mathtt{pref}(\overline{K}^c) \subseteq \sum_i (R_i S_i^o + R_i^{\leq})$$

$$\Rightarrow \quad K^c \subseteq \sum_i (R_i S_i^o + R_i^{\leq})$$

$$\text{iff} \quad \sum_i (R_i S_i^o + R_i^{\leq}) + K \text{ universal}$$

**Condition for $\mathtt{pref}(\overline{A}) \subseteq A$**

Equivalent to $A$ prefix close

**Condition for $K^c \subseteq \mathtt{pref}(\overline{K}^c)$**

Equivalent to $K$ saturated

# And with the arrow ?

The generalisation seems feasible but very technical.

## Only the arrow

1st issue: the dualities that have to be reported on the automaton.

2nd issue: the cap-links have to be slightly generalised.

## Both together

1st issue : Automaton on a for letter alphabet

2nd issue : cases where $* \to * \leq u \geq * \times *$ have to be tracked.

# Removing the saturation

## Another Decidable restriction from Priesnitz

Condition : the cap automaton is "deterministic"... Which is very restrictive (and false as stated in the thesis). But there are some interesting ideas.

## Look for a more abstract completion/topology

I already tried to use profinite topologies, but it did not work.
Maybe a combination with the actual result ? Or a kind of variant ?