Characterizing complexity classes with categorical logic

Complexity Days 2023

December 12, 2023

Damiano Mazza, & Baptiste Chanus

Descriptive complexity

Descriptive Complexity. Immerman (1999)

Example (Immerman 99)

For another example, consider the binary string $w = $ "01101". We can code w as the structure $A^w = (\{0, 1, \ldots, 4\}, \leq, \{1, 2, 4\})$ of vocabulary τ_s. Here $\leq$ represents the usual ordering on $0, 1, \ldots, 4$. Relation $S^w = \{1, 2, 4\}$ represents the positions where w is one.

Descriptive complexity

Descriptive Complexity. Immerman (1999)

Example (Immerman 99)

For another example, consider the binary string $w = $ "01101". We can code w as the structure $A^w = (\{0, 1, \ldots, 4\}, \leq, \{1, 2, 4\})$ of vocabulary τ_s. Here $\leq$ represents the usual ordering on $0, 1, \ldots, 4$. Relation $S^w = \{1, 2, 4\}$ represents the positions where w is one.

External axiomatization

Descriptive Complexity. Immerman (1999)

Example (Immerman 99)

Second-order logic consists of first-order logic plus new relation variables over which we may quantify. For example, the formula $(\forall A^r)\phi$ means that for all choices of r-ary relation A, ϕ holds.

Descriptive complexity

Descriptive Complexity. Immerman (1999)

Example (Immerman 99)

Second-order logic consists of first-order logic plus new relation variables over which we may quantify. For example, the formula $(\forall A^r)\phi$ means that for all choices of r-ary relation A, ϕ holds.

External to the language

1. Boolean Theories

Definition

A **Boolean theory** $\mathbb{T}$ is a triple

$$(\mathrm{Sort}(\mathbb{T}), \mathrm{Rel}(\mathbb{T}), \mathrm{Ax}(\mathbb{T}))$$

A Boolean theory $\mathbb{T}$ is **finite** if $\mathrm{Sort}(\mathbb{T})$, $\mathrm{Rel}(\mathbb{T})$ and $\mathrm{Ax}(\mathbb{T})$ are all finite.

Example : $\mathbb{S}\mathrm{tr}$

Definition

$$\begin{aligned} \mathrm{Sort}(\mathbb{S}\mathrm{tr}) &= \{N\} \\ \mathrm{Rel}(\mathbb{S}\mathrm{tr}) &= \{\leq \rightarrowtail N \times N, \mathrm{isOne} \rightarrowtail N\} \\ \mathrm{Ax}(\mathbb{S}\mathrm{tr}) &= \{\text{“} \leq \text{is a total order''}\} \end{aligned}$$

$$\begin{array}{ccccccccc} (N, \leq) & : & \mathsf{a} & \leq & \mathsf{b} & \leq & \mathsf{c} & \leq & \mathsf{d} \\ & & \uparrow & & \uparrow & & \uparrow & & \uparrow \\ \mathrm{isOne} & : & 0 & & 1 & & 0 & & 1 \end{array}$$

Extension of a theory

Definition

$\mathbb{T}$ extends $\mathbb{T}'$ iff :

- $\mathrm{Sort}(\mathbb{T}') \subseteq \mathrm{Sort}(\mathbb{T})$
- $\mathrm{Rel}(\mathbb{T}') \subseteq \mathrm{Rel}(\mathbb{T})$
- $\mathrm{Ax}(\mathbb{T}') \subseteq \mathrm{Ax}(\mathbb{T})$

Definition

$\mathbb{T}$ is a relational extension of $\mathbb{T}'$ iff :

- $\mathbb{T}'$ is an extension of $\mathbb{T}$
- $\mathrm{Sort}(\mathbb{T}') = \mathrm{Sort}(\mathbb{T})$

Fagin's Theorem (our version)

Theorem (Fagin (Boolean sauce))

NP is equal to the relational extensions of $\mathbb{S}\mathrm{tr}$.

Extending strings with table of symbols

$$\mathbb{S}\mathrm{tr} + \textbf{S,T} + \mathrm{Symb}_0, \mathrm{Symb}_1, \mathrm{Symb}_\square \rightarrowtail T \times S + (\mathrm{State}_q) \rightarrowtail T$$

Axioms :

- **S, T** are finite chains (equipped with successors and max)
- $\mathrm{Symb}_{\{0,1,\square\}}$ form a function from $T \times S$ to $\{0, 1, \square\}$ and $(State_q)$ from T to Q
- State q_0 and blank symbols $\square$ on work tape at time 0. State $accept$ at final state

i_0	i_1	i_2		i_{n-1}	i_n
0	0	1	...	0	0

	s_1	s_2	...	s_{n-1}	s_n	
t_1	1	1	...	0	0	q_0
t_2	0	1	...	0	1	q
$\vdots$			...			$\vdots$
t_{m-1}	1	0	...	0	0	q'
t_m	1	1	...	0	0	$accept$

Adding heads

$\mathbb{S}\mathrm{tr} + \textbf{S,T} + \mathrm{Symb}_{\{0,1,\square\}}, (\mathrm{State}_q) + \mathrm{wHead} \rightarrowtail T \times S + \mathrm{iHead} \rightarrowtail T \times N$

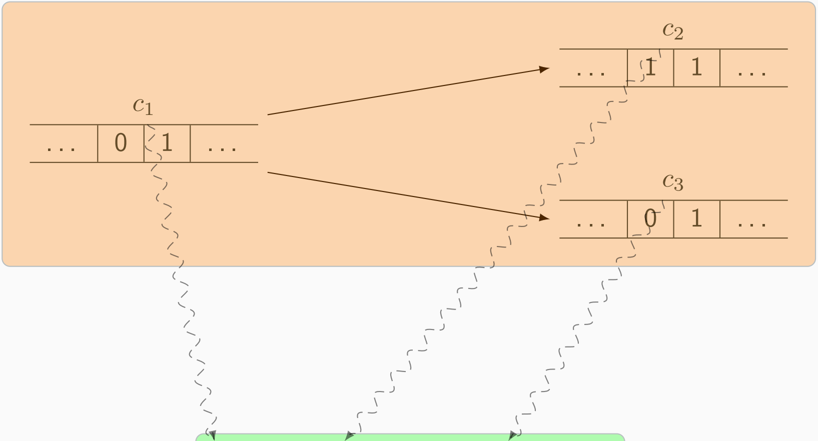
Axioms :

- wHead (resp. iHead) are functions from T to S (resp. N)
- wHead and iHead don't move more than one case
- The work tape is unchanged at positions where the head is not found

i_0	i_1	i_2		i_{n-1}	i_n
0	0	1	...	0	0

	s_1	s_2	...	s_{n-1}	s_n	
t_1	1	1	...	0	0	q_0
t_2	0	1	...	0	0	q
$\vdots$	$\vdots$	$\vdots$	...	$\vdots$	$\vdots$	$\vdots$
t_{m-1}	1	0	...	0	0	q'
t_m	1	1	...	0	1	$accept$

Axioms for the transitions



$$\Phi_{c_1}(t) \;\Rightarrow\; \Phi_{c_2}(t+1) \;\vee\; \Phi_{c_3}(t+1)$$

Polynomiality

All Turing mahines are represented !

But $\#T$ is exactly the time of the Turing machine.

If $\#T = \text{poly}(\#N)$ we can make the extension relational.

P class

Theorem (Grädel (Boolean sauce))

P is equal to the Horn extensions of $\mathbb{S}\mathrm{tr}$.

2. Classes of morphisms

Quick definitions

Definition (Category)

$\mathcal{C}$ a category is a collection of :

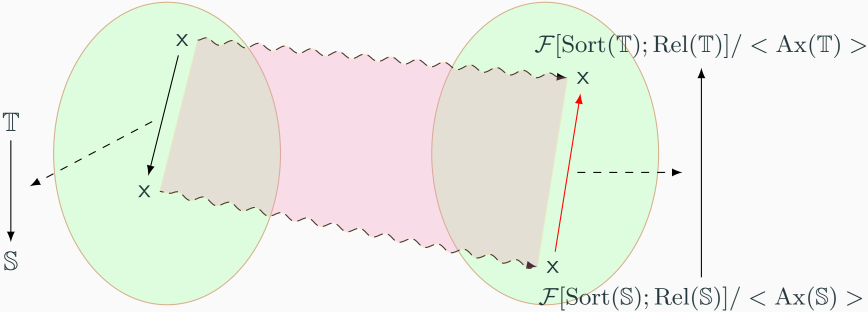
- Objects : $X, Y, \ldots$
- Morphisms : $f : X \to Y, \ldots$

With an associative composition between morphisms and identity morphisms for each object that are neutral for the composition.

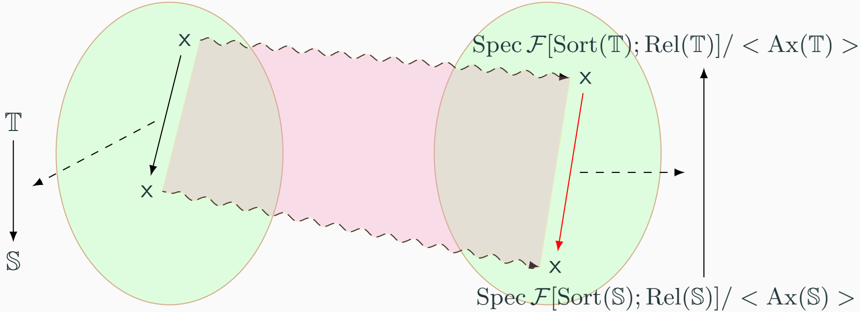
Definition (Functor)

A functor $F : \mathcal{C} \to \mathcal{D}$ is a mapping of objects and morphisms of $\mathcal{C}$ to objects and morphisms of $\mathcal{D}$ that preserves composition and identities.

$$\mathbf{BoolTh} \xrightarrow{\mathcal{F}[\_]} \mathbf{BoolCat}$$

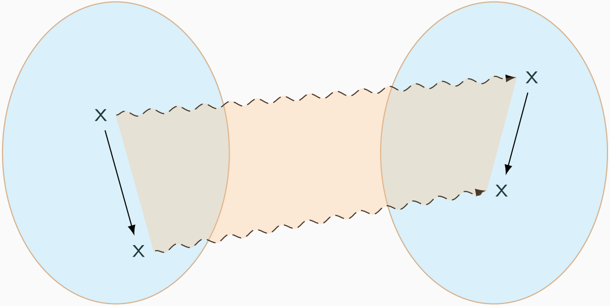


$$\mathbf{BoolTh} \xrightarrow{\operatorname{Spec}\mathcal{F}[\_]} \mathbf{BoolCat}^{op} \;:= \mathcal{D}ata$$



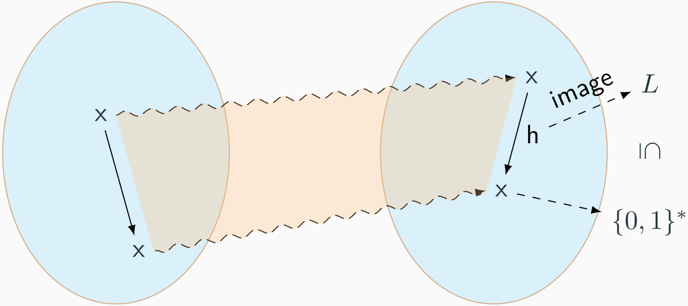
Characterization ?

$$\mathcal{C} \xrightarrow{\Gamma} \mathbf{Set}$$



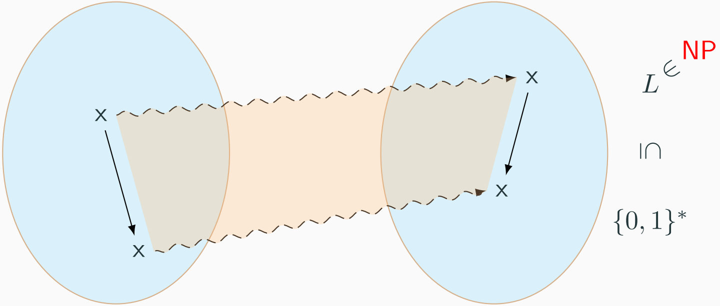
Characterization ?

$$\mathcal{C} \xrightarrow{\Gamma} \mathbf{Set}$$



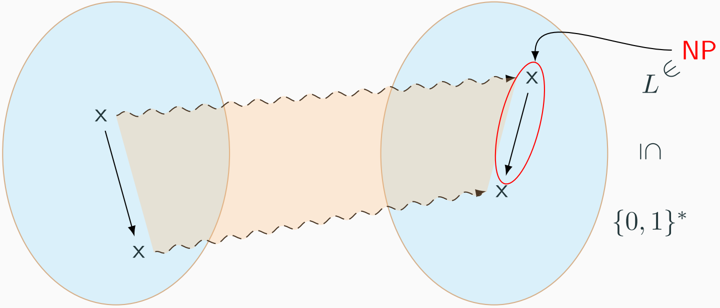
Characterization ?

$$\mathcal{C} \xrightarrow{\Gamma} \mathbf{Set}$$



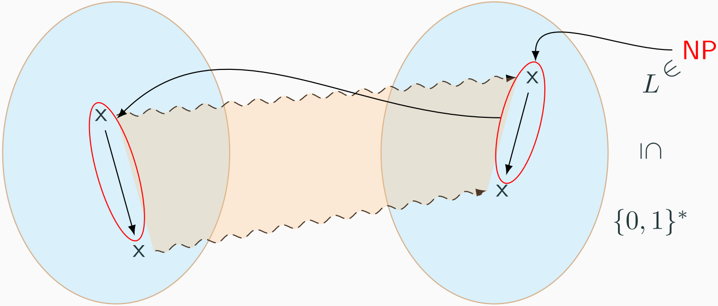
Characterization ?

$$\mathcal{C} \xrightarrow{\Gamma} \mathbf{Set}$$

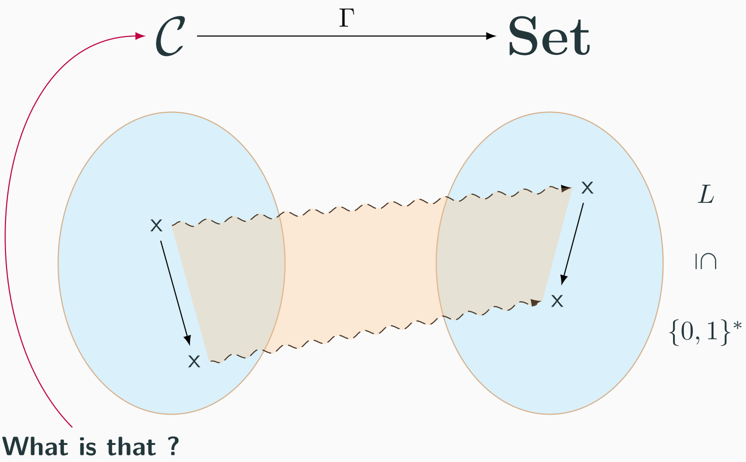


Characterization ?

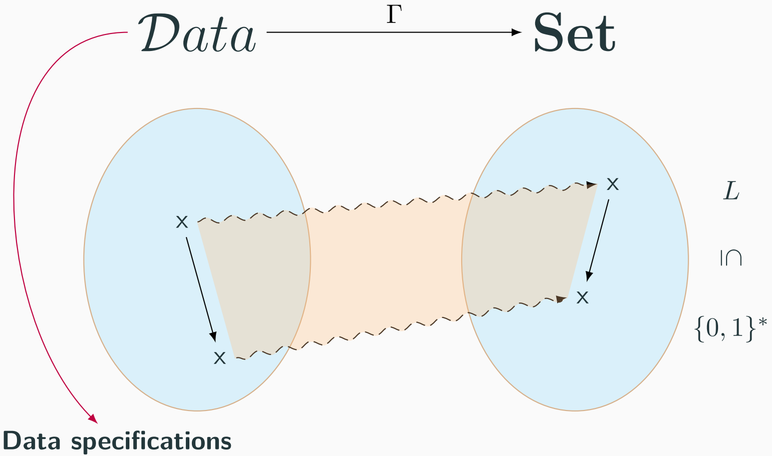
$$\mathcal{C} \xrightarrow{\Gamma} \mathbf{Set}$$



Characterization ?

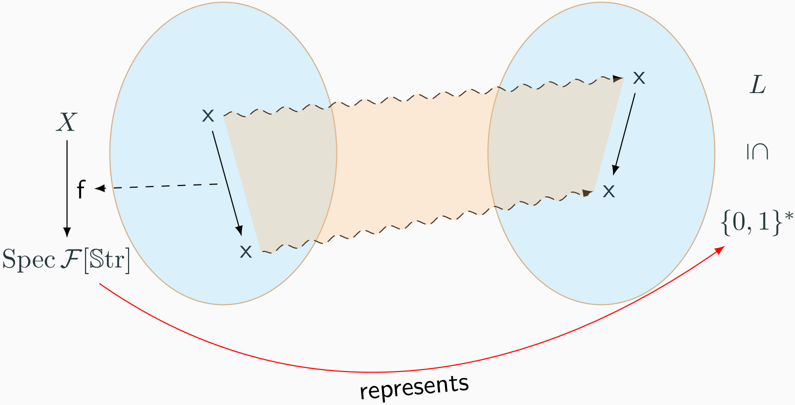


Characterization ?

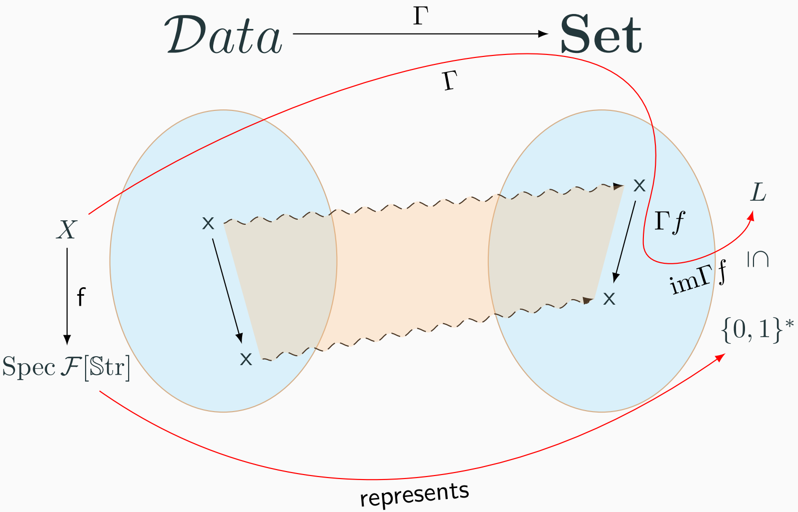


Characterization ?

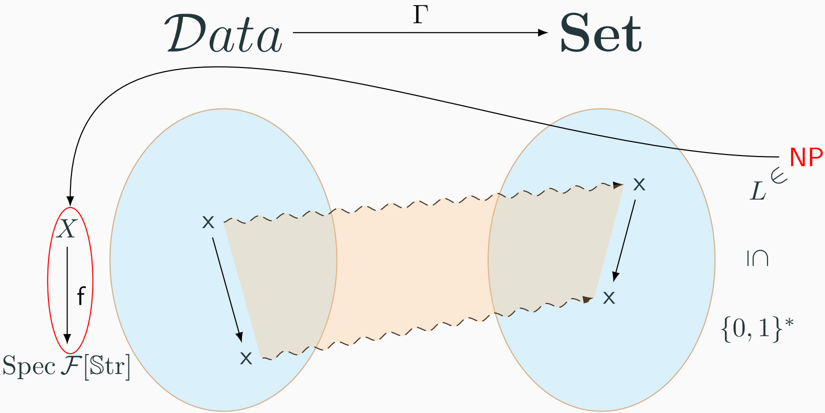
$$\mathcal{D}ata \xrightarrow{\Gamma} \mathbf{Set}$$



Characterization ?



Characterization ?



Fagin's Theorem (our version)

Theorem (Fagin (in $\mathcal{D}ata$))

A decision problem $L \subseteq \{0,1\}*$ is in NP iff it is expressible by a relational morphism on Str.

Theorem (Grädel (in $\mathcal{D}ata$))

A decision problem $L \subseteq \{0,1\}*$ is in P iff it is expressible by a Horn morphism on Str.

3. Proof of concept

Characterization of P/poly

Theorem (P/poly)

A decision problem $L \subseteq \{0,1\}^*$ is in P/poly iff it is expressible by a bounded Horn morphism of finite type on Str.

Finite type and presentation

Logical description

$\mathcal{F}[A_1, \ldots, A_n; R_1, \ldots, R_m]/ < \mathrm{Ax} >$

Algebraic geometry

$\mathcal{R}[X_1, \ldots, X_n]/I$

Finite

Finitely generated

Finite type

Finite presentation

Bounded morphism

Definition (Bounded morphism)

$f : X \to S$ is bounded if there exists presentations $\mathbb{S} \subseteq_{\mathrm{rel}} \mathbb{S}' \subseteq_{\mathrm{ax}} (\mathbb{S}_i)_{i \in \mathbb{N}^{\mathrm{Sort}(\mathbb{S})}}$ with $X = \operatorname{Spec} \mathcal{F}[\mathbb{S}'], S = \operatorname{Spec} \mathcal{F}[\mathbb{S}]$ and $m \in \mathbb{N}$ such that :

$$\forall i, |\mathrm{Ax}(\mathbb{S}_i') \backslash \mathrm{Ax}(\mathbb{S}')| \leq m$$

$$\begin{tikzcd}
X_0 \arrow[dr, "\mathrm{ax}"] & \dots \arrow[d, "\mathrm{ax}"] & X_i \arrow[dl, "\mathrm{ax}"] \\
& X \arrow[d, "\mathrm{rel}"] & \\
& S &
\end{tikzcd}$$

Conclusion

Theorem (P/poly)

A decision problem $L \subseteq \{0,1\}^*$ is in P/poly iff it is expressible by a bounded Horn morphism of finite type on Str.

No explicit reference to a polynom

- Can we find natural purely semantical characterizations ?
- Can the analogy with algebraic geometry give new tools to understand logical characterizations of complexity classes ?
- Can we generalize to theories other than $\mathbb{S}\mathrm{tr}$? (order independent characterizations)

Thank you !