Descriptive Complexity

and semantically defined

Fragments of Ptime

Martin Otto
RWTH Aachen
otto@informatik.rwth-aachen.de

London meeting, January 99

Descriptive Complexity

matching computational **complexity** & logical **definability**

"capturing complexity classes"

$$\mathcal{C} \equiv \mathsf{L}$$

complexity class — logic, *recursive syntax*

i.e. for all ($\simeq$-closed) classes K
of finite structures t.f.a.e.:

- K is $\mathcal{C}$-reconizable
- K is L-definable

(+ some no-nonsense conditions)

examples

Fagin

$$\mathrm{NP} \equiv \Sigma^1_1 \qquad \text{(all)}$$

Immerman, Vardi

$$\mathrm{Ptime} \equiv \mathrm{FP} \qquad \text{(ordered)}$$

Abiteboul, Vardi, Vianu

$$\mathrm{Pspace} \equiv \mathrm{PFP} \qquad \text{(ordered)}$$

Büchi, Elgot, Trakhtenbrot

$$\mathrm{REG} \equiv \mathrm{MSO} \qquad \text{(words)}$$

Order and the Problem of Genericity or Isomorphism Invariance

$\mathcal{A}$ recognizes a property of finite structures

$\Rightarrow$ $\mathcal{A}$ gives same result on
(different legal encodings of)
isomorphic inputs

$\boxed{\text{genericity} = \simeq\text{-invariance}}$

unproblematic in the presence of order:
canonical representations of the form $\big(n, <^n, \ldots\big)$
(easy canonization w.r.t. $\simeq$)

the abstract capturing issue

recursive syntax for a non-recursive class of algorithms [semantic constraint]

e.g.: Ptime/ $\simeq$

Ptime algorithms that accept an $\simeq$-closed class of structures

N.B.: Ptime itself is non-recursive

but admits recursive syntax through "polynomially clocked algorithms"

IF

finite graphs admitted Ptime canonization w.r.t. $\simeq$:

$$\mathsf{H}\colon \mathfrak{G} \longmapsto \mathsf{H}(\mathfrak{G}) = \Big(n, E\Big)$$

$$\begin{array}{ll} \text{s.t.} & \mathsf{H}(\mathfrak{G}) \simeq \mathfrak{G} \\ & \mathfrak{G} \simeq \mathfrak{G}' \Rightarrow \mathsf{H}(\mathfrak{G}) = \mathsf{H}(\mathfrak{G}') \end{array}$$

THEN (over graphs)

$$\mathsf{Ptime} \;\equiv\; \mathsf{Ptime} \circ \mathsf{H}$$

Ptime/$\simeq$

no semantic constraints
all polyn. clocked alg.

$\Rightarrow$ recursive syntax
a **logic for Ptime**

variations on the capturting issue

impose *stronger invariance condition*
w.r.t. an equivalence relation $\sim$
$\sim$ rougher than $\simeq$

to get fragments

$$\mathrm{Ptime}/{\sim} \quad \subseteq \quad \mathrm{Ptime}/{\simeq}$$

and try to capture

$$\boxed{\text{Ptime w.r.t. } {\sim}\text{-closed properties}}$$

Relevant Logics and Notions of Equivalence

failure of FO in descriptive complexity

- elementary equivalence = isomorphism
- no recursive mechanisms in FO

$$\text{FO} \;\text{———}\; \text{L}_{\infty[\omega]} \qquad\qquad \equiv_{(\infty)}$$

weak everything

$\rightarrow$ extensions with recursive mechanisms

least or inductive/partial fixed-point operators
FP/PFP

based on *inductive iteration* of
first-order predicate transformations

$$X \longmapsto \Big\{ \bar{x} \mid \varphi(X, \bar{x}) \Big\}$$

bounded-variable fragments

$$\mathsf{L}^k \quad \text{———} \quad \mathsf{L}^k_\infty \qquad\qquad \equiv^k_{(\infty)}$$

- only k variables, free or bound
- $\equiv^k$-classes non-trivial

$$\mathsf{FP} \;\subseteq\; \mathsf{PFP} \;\subsetneq\; \bigcup \mathsf{L}^k_\infty$$

$\rightarrow$ interesting recursion within k-variable strata

however, even in L^k_∞ lose grip on cardinalities, e.g. $\mathsf{L}^k_\infty \equiv \mathsf{L}^k$ trivial over pure sets.

adding cardinalities/counting on top

$$\mathsf{C}^k \;\text{———}\; \mathsf{C}^k_\infty \qquad\qquad \equiv^k_{C(\infty)}$$

- only k variables
- explicit *counting quantifiers* $\exists^{\geqslant m} x \ldots$ for all m

N.B.: $\exists^{\geqslant m} x \ldots$ in FO,
though not in general in L^k

examples (at the lower end)

- re-use of variables

$$\begin{aligned} & \exists y_1 \exists y_2 \exists y_3 \Big(Exy_1 \wedge Ey_1y_2 \wedge Ey_2y_3 \wedge Py_3 \Big) \\ \equiv \; & \exists y \Bigg(Exy \wedge \exists x \Big(Eyx \wedge \exists y (Exy \wedge Py) \Big) \Bigg) \end{aligned}$$

- $\mathsf{L}^2 \supsetneq \mathsf{ML}$ (modal logic)

$$\begin{aligned} \Big(\Diamond \varphi \Big)(x) \equiv \exists y \Big(Exy \wedge \varphi(y) \Big) \\ \Big(\Box \varphi \Big)(x) \equiv \forall y \Big(Exy \to \varphi(y) \Big) \end{aligned}$$

- $\equiv^2$-closed: wellfoundedness, wellorder property

- *not* $\equiv^2$-closed: transitivity, linear order property

expressive power of two variables, ctd.

- every finite ordered graph is characterised up to $\simeq$ by a single sentence of L^2 (after Poizat)
- almost every finite graph is characterised up to $\simeq$ by a single sentence of C^2 (Immerman,Lander; Babai, Erdös)
  – stable colouring in C^2
- each full binary tree of finite depth characterised in C^2, and in L^3, but not in L^2

The Modal Fragment

capturing, the way it should be

$$\text{Ptime}/\!\sim$$

$\sim$	modal equivalence bisimulation equivalence

$\text{Ptime}/\sim\; = \text{Ptime} \cap \text{ML}_\infty$

$\boxed{\text{the class of all } \sim\text{-closed Ptime properties of finite coloured graphs with distinguished nodes (Kripke structures)}}$

in the bisimulation invariant spectrum

$$\mathrm{ML} \;\; \frac{\quad}{}\!\!\overset{\mathsf{L}_\mu}{\bullet}\!\!\frac{\qquad\quad}{} \;\; \mathrm{ML}_\infty \qquad\qquad \sim$$

modal μ-calculus L_μ :

ML + monadic least fixed-points

$\mathsf{L}_\mu \subsetneq \mathrm{Ptime}/\!\sim$

as $\mathsf{L}_\mu \subseteq$ MSO and REG $\subsetneq$ Ptime over words

Ehrenfeucht-Fraïssé style analysis of bisimulation (in-)equivalence $\rightarrow$ reduction to ordered quotients

$$\sim \;=\; \bigcap \sim_n \qquad \not\sim \;=\; \bigcup \not\sim_n$$

(co-inductive) (inductive)

inductive refinement	$\not\sim_0 \subseteq \not\sim_1 \subseteq \cdots$	$\not\sim = \bigcup \not\sim_n$
+ order in the stages	$\prec_0 \subseteq \prec_1 \subseteq \cdots$	$\prec = \bigcup \prec_n$

$$(A,a) \; \underset{\prec_0}{\not\sim_0} \; (B,b) \quad \Leftrightarrow \quad \mathsf{atp}(a) \; \underset{<}{\neq} \; \mathsf{atp}(b)$$

$$(A,a) \; \underset{\prec_{n+1}}{\not\sim_{n+1}} \; (B,b) \quad \Leftrightarrow$$

$$(A,a) \; \underset{\prec_n}{\not\sim_n} \; (B,b)$$

$$\text{or} \quad E^A[a]/\sim_n \; \underset{\prec_{\mathrm{lex}}}{\neq} \; E^B[b]/\sim_n$$

the modal invariant

$$\mathrm{I}_<(\mathfrak{A}) := \mathfrak{A}/\!\sim\, = \Big(A/\!\sim, <, E^\sim, \ldots\Big)$$

where $\quad ([a_1],[a_2]) \in E^\sim \;\Leftrightarrow\; E[a_1] \cap [a_2] \neq \emptyset$

identifying $\Big(A/\!\sim, <, \ldots\Big)$ with standardised $\Big(n, \ldots\Big)$

obtain a *complete invariant* w.r.t. $\sim$:

$$\mathrm{I}\colon \mathfrak{A} \longmapsto \mathrm{I}(\mathfrak{A})$$

s.t. $\quad \mathfrak{A} \sim \mathfrak{B} \;\Leftrightarrow\; \mathrm{I}(\mathfrak{A}) = \mathrm{I}(\mathfrak{B})$

indeed, moreover $\quad \boxed{\mathrm{I}(\mathfrak{A}) \sim \mathfrak{A}}$

whence I provides *canonization* w.r.t. $\sim$

N.B.: $\quad \mathfrak{A} \mapsto \mathrm{I}(\mathfrak{A})$ is in Ptime

the capturing result

$$\text{Ptime}/\!\sim\; \equiv\; \text{Ptime} \circ \mathrm{I} \;\equiv\; \text{FP} \circ \mathrm{I}$$

$<$ FP-definable over I

remarks

- quotients w.r.t. $\sim$ *are* the hereditarily finite sets in AFA set theory
- concrete syntax: a higher-dimensional μ-calculus

straightforward extensions cover

- multi-modal case
- graded bisimulation (counting multiplicities)

Invariants for $\equiv^k_C$
abstracted from k-pebble games

Ehrenfeucht-Fraïssé games
with only k marked elements per structure
relocation instead of addition

Barwise,Poizat,Immerman: k-pebble game

Immerman,Lander: k-pebble game with counting

$\mathfrak{A} \equiv^k \mathfrak{B} \quad \Leftrightarrow$
second player has a winning strategy
in the k-pebble game over $\mathfrak{A}$ and $\mathfrak{B}$

[similarly with counting]

coding the game as a Kripke structure

positions over $\mathfrak{A}$:	A^k
moving pebble i:	$E_i = \big\{(\bar{a}, \bar{a}') \mid a_j = a'_j \text{ for } j \neq i\big\}$
basic condition:	atp($\bar{a}$) agree

Put $$\mathfrak{A}^k := \big(A^k, E_1, \dots, E_k, (P_\theta)_{\theta \text{atp}}\big)$$

to find that

$$\begin{array}{ll} & \mathfrak{A} \equiv^k \mathfrak{B} \\ \Leftrightarrow & \textbf{II} \text{ has winning strategy on } \mathfrak{A}, \mathfrak{B} \\ \Leftrightarrow & \mathfrak{A}^k \sim \mathfrak{B}^k \\ \Leftrightarrow & \mathrm{I}(\mathfrak{A}^k) = \mathrm{I}(\mathfrak{B}^k) \end{array}$$

$\rightarrow$ complete invariants w.r.t. $\equiv^k$ in Ptime

$$\mathrm{I}^{\mathsf{k}}(\mathfrak{A}) := \mathrm{I}(\mathfrak{A}^k)$$

[$\mathrm{I}^{\mathsf{k}}_{\mathsf{C}}$ for $\equiv^k_C$ similarly via graded bisimulation]

Computational Adequacy of the Invariants

recall that $\mathsf{FP} \subseteq \mathsf{PFP} \subsetneq \bigcup L^k_\infty$

a piece of "reverse" descriptive complexity

$$\mathsf{FP} \equiv \bigcup \mathsf{Ptime} \circ \mathrm{I}^{\mathsf{k}}$$

$$\mathsf{PFP} \equiv \bigcup \mathsf{Pspace} \circ \mathrm{I}^{\mathsf{k}}$$

Abiteboul-Vianu Theorem

$$\mathsf{FP} \equiv \mathsf{PFP} \quad \Leftrightarrow \quad \mathsf{Ptime} = \mathsf{Pspace}$$

[the same goes for the counting extensions]

in the modal scenario:

$\mathrm{I}(\mathfrak{A})$ *is* itself a structure equivalent with $\mathfrak{A}$

in the k-variable scenario:

$\mathrm{I}^{\mathsf{k}}(\mathfrak{A}) = \mathrm{I}(\mathfrak{A}^k)$ is a structure
characterising the game over $\mathfrak{A}$

canonization w.r.t. $\equiv^k$ would mean to find
$\mathfrak{B}$ s.t. $\mathfrak{B}^k \sim \mathfrak{A}^k$
rather than just
$\mathfrak{C}$ s.t. $\mathfrak{C} \sim \mathfrak{A}^k$

$\rightarrow$ issue of *inversion* of the invariants general situation: $\approx$ equivalence over D

complete invariant

$$\mathsf{I}\colon D \to S \quad \text{s.t. } d \approx d' \;\Leftrightarrow\; \mathsf{I}(d) = \mathsf{I}(d')$$

canonization

$$\mathsf{H}\colon D \to D \quad \text{s.t. } \begin{array}{l} \mathsf{H}(d) \approx d \\ d \approx d' \;\Rightarrow\; \mathsf{H}(d) = \mathsf{H}(d') \end{array}$$

inversion of invariant I

$$\mathsf{F}\colon S \to D \quad \text{s.t. } \mathsf{I} \circ \mathsf{F} = \mathsf{id}_S$$

general situation

$$\begin{array}{ll} & \text{Ptime canonization} \\ \Rightarrow & \text{Ptime invariant} \\ \Rightarrow & \text{equivalence in Ptime} \end{array}$$

Blass, Gurevich: that is all, in the general case,
unless complexity collapses happen

---

little is known for concrete equivalences, e.g.

Gurevich: Ptime invariant for $\simeq$ would imply
Ptime canonization w.r.t. $\simeq$

All is Well for Two

Theorem
I^2 and I^2_C admit Ptime inversion

through combinatorial reconstruction of some $\mathfrak{A} = \Big(n, \dots\Big)$ from its game characteristic $\mathrm{I}^2_{(C)}$

consistent and *symmetry respecting* allocation of 2-types according to $\mathrm{I}^2_{(C)}$

for I^2 (without counting): guess multiplicities

for I^2_C (with counting): know multiplicities and satisfy additional summation equations

What is So Special About Two

for I^{k} (without counting)

Ptime inversion is too restrictive

impossible for $k \geqslant 3$:
$\mathrm{I}^3(\mathfrak{A})$ may be logarithmically smaller than $\mathfrak{A}$

unnecessary if Ptime canonization is the goal:
polynomiality in the result suffices

two questions

- is I^{k} even recursively invertible?
- can $\equiv^k$ have Ptime canonization
  (other than through complexity collapses)?

negative answers in the case without counting (**Martin Grohe**)

---

1. can code Diophantine equations through conditions on predicate cardinalities, s.t.

   I^3 specification forces equations to hold, without giving away solutions

   $\rightarrow$ not even recursive inversion

2. non-uniform self-reduction arguments based on canonization for 3-SAT

   $\rightarrow$ no Ptime canonization
   unless collapses happen

---

bad luck, if you cannot count

what if you can count

- we have Ptime computable complete invariants w.r.t. $\equiv_C^k$ for all k
- sizes well balanced
- invariants trivially invertible in NP
- if any one $\equiv_C^k$, $k \geqslant 3$,

  admits Ptime canonization, then

$$\bigcup \mathsf{Ptime}/{\equiv_C^k} \quad \equiv \quad \mathsf{FP}_C$$

- Ptime invertibility or canonization **OPEN**:

  Grohe's results precisely play on *inexpressibility of cardinalities*