Symmetric Computation: Lecture 2

Anuj Dawar and Gregory Wilsenach

Department of Computer Science and Technology, University of Cambridge

ESSLLI, August 2021

Descriptive Complexity

Descriptive Complexity provides an alternative perspective on Computational Complexity.

Computational Complexity

- Measure use of resources (space, time, *etc.*) on a machine model of computation;
- Complexity of a language—i.e. a set of strings.

Descriptive Complexity

- Complexity of a class of structures—e.g. a collection of graphs.
- Measure the complexity of describing the collection in a formal logic, using resources such as variables, quantifiers, higher-order operators, *etc.*

There is a fascinating interplay between the views.

Fagin's Theorem

Theorem (Fagin)
A class $\mathcal{C}$ of finite structures is definable by a sentence of *existential second-order logic* if, and only if, it is decidable by a *nondeterminisitic machine* running in polynomial time.

$$\mathsf{ESO} = \mathsf{NP}$$

Fagin's Theorem

If φ is $\exists R_1 \cdots \exists R_m \theta$ for a *first-order* θ.

To decide $\mathbb{A} \models \varphi$, *guess* an interpretation for the relations $R_1, \ldots, R_m$ and then evaluate θ in the expanded structure.

Given a *nondeterministic* machine M and a polynomial p:

$\exists \leq$ *a linear order*

$\exists H, T, S$ *that code an accepting computation of* M *of length* p *starting with* $[\mathbb{A}]_{\leq}$.

Is there a logic for P?

The major open question in *Descriptive Complexity* (first asked by Chandra and Harel in 1982) is whether there is a logic $\mathcal{L}$ such that

> *for any class of finite structures $\mathcal{C}$, $\mathcal{C}$ is definable by a sentence of $\mathcal{L}$ if, and only if, $\mathcal{C}$ is decidable by a deterministic machine running in polynomial time.*

Formally, we require $\mathcal{L}$ to be a *recursively enumerable* set of sentences, with a computable map taking each sentence to a Turing machine M and a polynomial time bound p such that (M, p) accepts a *class of structures*.

(Gurevich 1988)

Inductive Definitions

Let $\varphi(R, x_1, \ldots, x_k)$ be a first-order formula in the vocabulary $\sigma \cup \{R\}$
Associate an operator Φ on a given σ-structure $\mathbb{A}$:

$$\Phi(R^{\mathbb{A}}) = \{\mathbf{a} \mid (\mathbb{A}, R^{\mathbb{A}}, \mathbf{a}) \models \varphi(R, \mathbf{x})\}$$

We define the *non-decreasing* sequence of relations on $\mathbb{A}$:

$$\Phi^0 = \emptyset$$

$$\Phi^{m+1} = \Phi^m \cup \Phi(\Phi^m)$$

The *inflationary fixed point* of Φ is the limit of this sequence.
On a structure with n elements, the limit is reached after at most n^k stages.

FP

The logic FP is formed by closing first-order logic under the rule:

If φ is a formula of vocabulary $\sigma \cup \{R\}$ then $[\mathbf{ifp}_{R,\mathbf{x}}\varphi](\mathbf{t})$ is a formula of vocabulary σ.

The formula is read as:

the tuple $\mathbf{t}$ is in the inflationary fixed point of the operator defined by φ

LFP is the similar logic obtained using *least fixed points* of *monotone* operators defined by *positive* formulas.

LFP and FP have the same expressive power **(Gurevich-Shelah 1986; Kreutzer 2004)**.

Transitive Closure

The formula

$$[\mathbf{ifp}_{T,xy}(x = y \lor \exists z(E(x,z) \land T(z,y)))](u,v)$$

defines the *transitive closure* of the relation E

The expressive power of FP properly extends that of first-order logic.

Still, every property definable in FP is decidable in *polynomial time*.

On a structure with n elements, the fixed-point of an induction of arity k is reached in at most n^k steps.

Immerman-Vardi Theorem

Theorem

On structures which come equipped with a linear order FP *expresses exactly the properties that are in* P*.*

(Immerman; Vardi 1982)

Recall from *Fagin's theorem*:

> $\exists \leq$ *a linear order*
> $\exists H, T, S$ *that code an accepting computation of* M *of length* p *starting with* $[\mathbb{A}]_{\leq}$.

FP vs. Ptime

The order cannot be built up inductively.
It is an open question whether a *canonical* string representation of a structure can be constructed in polynomial-time.

If it can, there is a logic for P.
If not, then $P \neq NP$.

All P classes of structures can be expressed by a sentence of FP with $<$, which is invariant under the choice of order. The set of all such sentences is not *r.e.*

FP by itself is too weak to express all properties in P.
Evenness is not definable in FP.

Finite Variable Logic

We write L^k for the first order formulas using only the variables $x_1, \ldots, x_k$.

$$(\mathbb{A}, \mathbf{a}) \equiv^{L^k} (\mathbb{B}, \mathbf{b})$$

denotes that there is no formula φ of L^k such that $\mathbb{A} \models \varphi[\mathbf{a}]$ and $\mathbb{B} \not\models \varphi[\mathbf{b}]$

If $\varphi(R, \mathbf{x})$ has k variables all together, then each of the relations in the sequence:

$\Phi^0 = \emptyset$; $\Phi^{m+1} = \Phi^m \cup \Phi(\Phi^m)$

is definable in L^{2k}.

Proof by induction, using *substitution* and *renaming* of bound variables.

Examples

Connectivity is axiomatizable in L^k (for $k \geq 3$).
Even cardinality is *not*.

Connectivity in L^4:

$$\mathrm{path}_{\leq l}(x,y) := \exists z_1(E(x,z_1) \wedge \exists z_2(E(z_1,z_2) \wedge \exists z_1(E(z_2,z_1) \wedge \cdots E(z_i,y))))$$

$$\mathrm{disconnect}_l := \forall x,y(\mathrm{path}_{\leq l+1}(x,y) \Rightarrow \mathrm{path}_{\leq l}(x,y)) \wedge \exists x,y \neg \mathrm{path}_{\leq l}(x,y)$$

Connectivity is then axiomatized by the set

$$\{\neg \mathrm{disconnect}_l \mid l \in \mathbb{N}\}$$

Pebble Game

The k-pebble game is played on two structures $\mathbb{A}$ and $\mathbb{B}$, by two players—*Spoiler* and *Duplicator*—using k pairs of pebbles $\{(a_1, b_1), \ldots, (a_k, b_k)\}$.

> *Spoiler* moves by picking a pebble and placing it on an element (a_i on an element of $\mathbb{A}$ or b_i on an element of $\mathbb{B}$).
>
> *Duplicator* responds by picking the matching pebble and placing it on an element of the other structure
>
> *Spoiler* wins at any stage if the partial map from $\mathbb{A}$ to $\mathbb{B}$ definedby the pebble pairs is not a partial isomorphism
>
> *If Duplicator has a winning strategy for q moves, then $\mathbb{A}$ and $\mathbb{B}$ agree on all sentences of L^k of quantifier rank at most q.*
>
> **(Barwise)**

$\mathbb{A} \equiv^{L^k} \mathbb{B}$ if, for every q, *Duplicator* wins the q round, k pebble game on $\mathbb{A}$ and $\mathbb{B}$. Equivalently (on finite structures) *Duplicator* has a strategy to play forever.

Evenness

To show that *Evenness* is not definable in FP, it suffices to show that:

> *for every k, there are structures $\mathbb{A}_k$ and $\mathbb{B}_k$ such that $\mathbb{A}_k$ has an even number of elements, $\mathbb{B}_k$ has an odd number of elements and*
>
> $$\mathbb{A} \equiv^{L^k} \mathbb{B}.$$

It is easily seen that *Duplicator* has a strategy to play forever when one structure is a set containing k elements (and no other relations) and the other structure has $k+1$ elements.

Take $K_{k,k}$—the complete bipartite graph on two sets of k vertices.
and $K_{k,k+1}$—the complete bipartite graph on two sets, one of k vertices, the other of $k+1$.

These two graphs are $\equiv^{L^k}$ equivalent, yet one has a perfect matching, and the other does not.

Inexpressibility in FP

The following are not definable in FP:

- *Evenness*;
- *Perfect Matching*;
- *Hamiltonicity*.

The examples showing these inexpressibility results all involve some form of *counting*.

Fixed-point Logic with Counting

Immerman proposed FPC—the extension of FP with a mechanism for *counting*

Two sorts of variables:

- $x_1, x_2, \ldots$ range over $|A|$—the domain of the structure;
- $\nu_1, \nu_2, \ldots$ which range over *non-negative integers*.

If $\varphi(x)$ is a formula with free variable x, then $\#x\varphi$ is a *term* denoting the *number* of elements of $\mathbb{A}$ that satisfy φ.

We have arithmetic operations $(+, \times)$ on *number terms*.

Quantification over number variables is *bounded*: $(\exists \nu < t)\, \varphi$

Examples

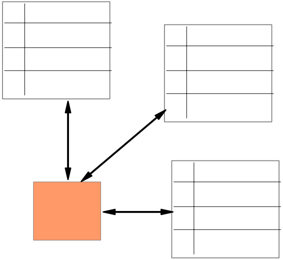
The following formula is true in a graph if, and only if, it has an even number of edges.

$$\begin{aligned}\exists \nu_1 \leq \#x(x = x)\ \exists \nu_2 \leq \nu_1 \times \nu_1\ &(\nu_1 = \#x(x = x))\wedge \\ &\nu_2 = \textstyle\sum_{\mu < \nu_1} \mu \times (\#x(\#yE(x, y) = \mu)) \\ &\exists \nu_3 \leq \nu_2(\nu_3 \times 4 = \nu_2)\end{aligned}$$

where the sum in the second line can be expressed using the fixed-point operator.

$$\begin{aligned}\mathbf{ifp}_{T,\mu,\tau}[&\mu = 0 \wedge \tau = \#x(\forall y \neg E(x, y))\vee \\ &\exists \mu' \leq \mu \exists \tau' \leq \tau(\mu = \mu' + 1 \wedge T(\mu', \tau')\wedge \\ &\quad \tau = \tau' + \mu \times \#x(\#yE(x, y) = \mu))](\nu_1, \nu_2).\end{aligned}$$

Relational Machines



Input: A relational database

Store: relational and numerical registers

Operations: *join, projection, complementation, counting*

Properites expressible in FPC are *exactly* those decidable by such a machine in *polynomial time*.

Expressive Power of FPC

Most *"obviously"* polynomial-time algorithms can be expressed in FPC.

This includes P-complete problems such as

CVP—*the Circuit Value Problem*
Input: a circuit, i.e. a labelled DAG with source labels from $\{0,1\}$*, internal node labels from* $\{\vee,\wedge,\neg\}$*.*
Decide: what is the value at the output gate.

CVP is expressible in FPC.

It is expressible in FPC also for circuits that may include *threshold or counting gates*.

Expressive Power of FPC

Many non-trivial polynomial-time algorithms can be expressed in FPC:

FPC captures all of P over any *proper minor-closed class of graphs*

(Grohe 2010)

But some cannot be expressed:

- There are polynomial-time decidable properties of graphs that are not definable in FPC. **(Cai, Fürer, Immerman, 1992)**
- *XOR-Sat*, or more generally, solvability of a system of linear equations over a finite field cannot be expressed in FPC. **(Atserias, Bulatov, D. 2009)**

Some NP-complete problems are *provably* not in FPC, including *Sat*, *Hamiltonicity* and *3-colouraiblity*.

Counting Quantifiers

C^k is the logic obtained from *first-order logic* by allowing:

- *counting quantifiers*: $\exists^i x\, \varphi$; and
- only the variables $x_1, \ldots . x_k$.

Every formula of C^k is equivalent to a formula of first-order logic, albeit one with more variables.

For every sentence φ of FPC, there is a k such that if $\mathbb{A} \equiv^{C^k} \mathbb{B}$, then

$$\mathbb{A} \models \varphi \quad \text{if, and only if,} \quad \mathbb{B} \models \varphi.$$

Weisfeiler-Leman Equivalences

$G \equiv^{C^k} H$ iff G and H cannot be distinguished by a sentence of first-order logic with *counting quantifiers* using only k variables.

$G \equiv^{C^{k+1}} H$ iff G and H are not distinguished by the coarsest partition of the k-tuples of G into classes $P_1, \ldots, P_t$ satisfying:

> *two tuples $\mathbf{u}$ and $\mathbf{v}$ in the same class P_i cannot be distinguished by counting the number of substitutions we can make in them to get a tuple in class P_j.*

Weisfeiler-Leman Equivalences

The k*-dimensional Weisfeiler-Leman* equivalence relation is an *overapproximation* of the isomorphism relation.

If G, H are n-vertex graphs and $k < n$, we have:

$$G \cong H \quad \Leftrightarrow \quad G \equiv^n H \quad \Rightarrow \quad G \equiv^{k+1} H \quad \Rightarrow \quad G \equiv^k H.$$

$G \equiv^k H$ is decidable in time $n^{O(k)}$.

It has many equivalent characterisations arising from

- *combinatorics* **(Babai)**
- *logic* **(Immerman-Lander)**
- *algebra* **(Weisfeiler; Holm)**
- *linear optimization* **(Atserias-Maneva; Malkin)**

Counting Game

Immerman and Lander (1990) defined a *pebble game* for C^k.
This is again played by *Spoiler* and *Duplicator* using k pairs of pebbles $\{(a_1, b_1), \ldots, (a_k, b_k)\}$.

> *At each move, Spoiler picks i and a set of vertices of one structure (say $X \subseteq B$)*
>
> *Duplicator responds with a set of vertices of the other structure (say $Y \subseteq A$) of the same size.*
>
> *Spoiler then places a_i on an element of Y and Duplicator must place b_i on an element of X.*
>
> *Spoiler wins at any stage if the partial map from $\mathbb{A}$ to $\mathbb{B}$ defined by the pebble pairs is not a partial isomorphism*
>
> *If Duplicator has a winning strategy for p moves, then $\mathbb{A}$ and $\mathbb{B}$ agree on all sentences of C^k of quantifier rank at most p.*

Bijection Games

$\equiv^{C^k}$ is also characterised by a k-pebble *bijection game*. **(Hella 96)**.
The game is played on structures $\mathbb{A}$ and $\mathbb{B}$ with pebbles $a_1, \ldots, a_k$ on $\mathbb{A}$ and $b_1, \ldots, b_k$ on $\mathbb{B}$.

- *Spoiler* chooses a pair of pebbles a_i and b_i;
- *Duplicator* chooses a bijection $h : A \to B$ such that for pebbles a_j and $b_j (j \neq i)$, $h(a_j) = b_j$;
- *Spoiler* chooses $a \in A$ and places a_i on a and b_i on $h(a)$.

Duplicator loses if the partial map $a_i \mapsto b_i$ is not a partial isomorphism.
Duplicator has a strategy to play forever if, and only if, $\mathbb{A} \equiv^{C^k} \mathbb{B}$.

Equivalence of Games

It is easy to see that a winning strategy for *Duplicator* in the bijection game yields a winning strategy in the counting game:

> *Respond to a set* $X \subseteq A$ *(or* $Y \subseteq B$*) with* $h(X)$ *(*$h^{-1}(Y)$*, respectively).*

For the other direction, consider the partition induced by the equivalence relation

$$\{(a, a') \mid (\mathbb{A}, \mathbf{a}[a/a_i]) \equiv^{C^k} (\mathbb{A}, \mathbf{a}[a'/a_i])\}$$

and for each of the parts X, take the response Y of *Duplicator* to a move where *Spoiler* would choose X.
Stitch these together to give the bijection h.

Cai-Fürer-Immerman Graphs

Cai-Fürer-Immerman show that there is a polynomial-time graph property that is not in FPC by constructing a sequence of pairs of graphs $G_k, H_k (k \in \omega)$ such that:

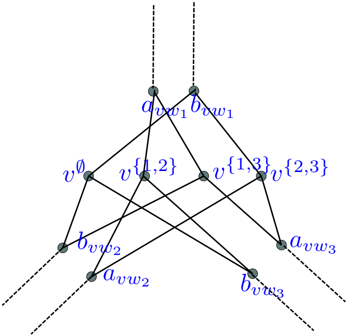
- $G_k \equiv^{C^k} H_k$ for all k.
- There is a polynomial time decidable class of graphs that includes all G_k and excludes all H_k.

In particular, the first point shows that $\equiv^{C^k}$ (for any fixed k) does not capture isomorphism everywhere

Constructing G_k and H_k

Given any graph G, we can define a graph X_G by replacing every edge with a pair of edges, and every vertex with a gadget.

The picture shows the gadget for a vertex v that is adjacent in G to vertices w_1, w_2 and w_3.
The vertex v^S is adjacent to $a_{vw_i} (i \in S)$ and $b_{vw_i} (i \notin S)$ and there is one vertex for all *even size* S.
The graph $\tilde{X}_G$ is like X_G except that at *one vertex* v, we include v^S for *odd size* S.



Properties

If G is *connected* and has *treewidth* at least k, then:

1. $X_G \not\cong \tilde{X}_G$; and
2. $X_G \equiv^{C^k} \tilde{X}_G$.

(1) allows us to construct a polynomial time property separating X_G and $\tilde{X}_G$.
(2) is proved by a game argument.

> *The original proof of* **(Cai, Fürer, Immerman)** *relied on the existence of balanced separators in* G. *The characterisation in terms of treewidth is from* **(D., Richerby 07)**.