Descriptive Polynomial Time Complexity

Tutorial Part 3

Anuj Dawar
University of Cambridge

Prague Fall School, 22 September 2011

Recapitulation

By Fagin's theorem, a class of finite structures is definable in *existential second-order logic* if, and only if, it is in NP.

It is an open question whether there is similarly a logic for PTime.

This is equivalent to the question of whether there is a problem in PTime that is complete under *first-order reductions*.

Recapitulation II

IFP extends first-order logic with *inflationary fixed-points*.

By the theorem of Immerman and Vardi, it captures PTime on *ordered structures*, but is too weak without order.

IFP + C extends IFP with *counting*.

It forms a natural expressivity class *properly* contained in PTime.

Note: If there is a PTime-complete problem under IFP + C-reductions, then there is a logic for PTime.

Cai-Fürer-Immerman Graphs

There are polynomial-time decidable properties of graphs that are not definable in IFP $+$ C. **(Cai, Fürer, Immerman, 1992)**

More precisely, we can construct 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.

Still, IFP $+$ C is a *natural* level of expressiveness within PTime.

Restricted Graph Classes

If we restrict the class of structures we consider, IFP $+$ C may be powerful enough to express all polynomial-time decidable properties.

1. IFP $+$ C captures PTime on *trees*. **(Immerman and Lander 1990)**.
2. IFP $+$ C captures PTime on any class of graphs of *bounded treewidth*. **(Grohe and Mariño 1999)**.
3. IFP $+$ C captures PTime on the class of *planar graphs*. **(Grohe 1998)**.
4. IFP $+$ C captures PTime on any *proper minor-closed class of graphs*. **(Grohe 2010)**.

In each case, the proof proceeds by showing that for any G in the class, a *canonical, ordered* representaton of G can be interpreted in G using IFP $+$ C.

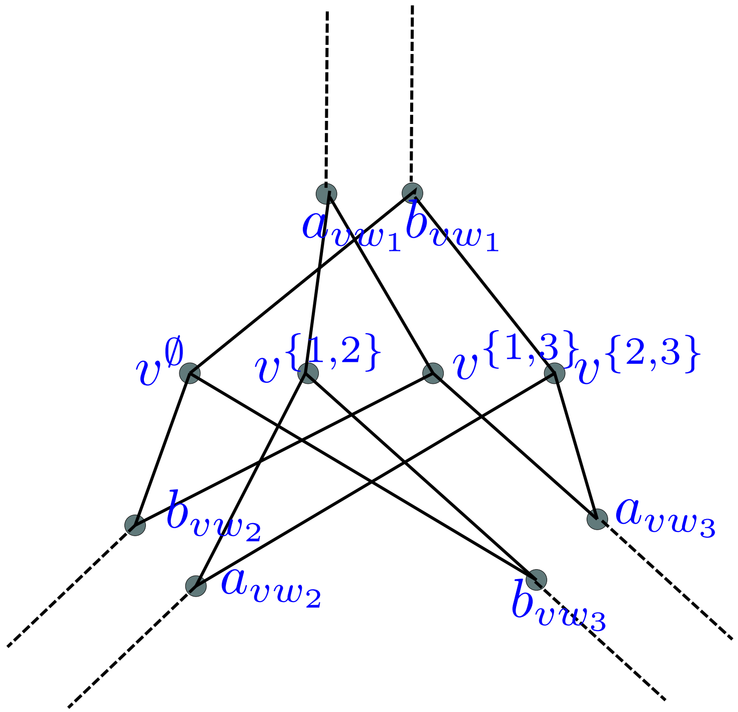
Constructing G_k and H_k

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)**.

Undefinability Results for IFP $+$ C

Other undefinability results for IFP $+$ C have been obtained:

- Isomorphism on *multipedes*—a class of structures defined by **(Gurevich-Shelah 96)** to exhibit a *first-order definable* class of *rigid* structures with no order definable in IFP $+$ C.
- 3-colourability of graphs. **(D. 1998)**

Both proofs rely on a construction very similar to that of Cai-Fürer-Immerman.

Question: Is there a natural polynomial-time computable property that is not definable in IFP $+$ C?

Solvability of Linear Equations

More recently it has been shown that the problem of solving linear equations over the two element field $\mathbb{Z}_2$ is not definable in $\mathrm{IFP} + \mathrm{C}$. **(Atserias, Bulatov, D. 09)**

The question arose in the context of classification of *Constraint Satisfaction Problems*.

The problem is clearly solvable in polynomial time by means of Gaussian elimination.

> We see how to represent systems of linear equations as *unordered* relational structures.

Systems of Linear Equations

Consider structures over the domain $\{x_1, \ldots, x_n, e_1, \ldots, e_m\}$, (where $e_1, \ldots, e_m$ are the equations) with relations:

- unary E_0 for those equations e whose r.h.s. is 0.
- unary E_1 for those equations e whose r.h.s. is 1.
- binary M with $M(x, e)$ if x occurs on the l.h.s. of e.

Solv$(\mathbb{Z}_2)$ is the class of structures representing solvable systems.

Undefinability in IFP $+$ C

Take $\mathcal{G}$ a 3-regular, connected graph with treewidth $> k$.

Define equations $\mathbf{E}_{\mathcal{G}}$ with two variables x_0^e, x_1^e for each edge e.

For each vertex v with edges e_1, e_2, e_3 incident on it, we have eight equations:

$$E_v: \qquad x_a^{e_1} + x_b^{e_2} + x_c^{e_3} \equiv a + b + c \pmod 2$$

$\tilde{\mathbf{E}}_{\mathcal{G}}$ is obtained from $\mathbf{E}_{\mathcal{G}}$ by replacing, for exactly one vertex v, E_v by:

$$E_v': \qquad x_a^{e_1} + x_b^{e_2} + x_c^{e_3} \equiv a + b + c + 1 \pmod 2$$

We can show: $\mathbf{E}_{\mathcal{G}}$ is satisfiable; $\tilde{\mathbf{E}}_{\mathcal{G}}$ is unsatisfiable; $\mathbf{E}_{\mathcal{G}} \equiv^{C^k} \tilde{\mathbf{E}}_{\mathcal{G}}$

Satisfiability

Lemma $\mathbf{E}_G$ is satisfiable.

by setting the variables x_i^e to i.

Lemma $\tilde{\mathbf{E}}_G$ is unsatisfiable.

Consider the subsystem consisting of equations involving only the variables x_0^e.

The sum of all *left-hand sides* is

$$2\sum_e x_0^e \equiv 0 \pmod 2$$

However, the sum of *right-hand sides* is 1.

Bijection Games

$\equiv^{C^k}$ is 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 $\mathbb{B}$.

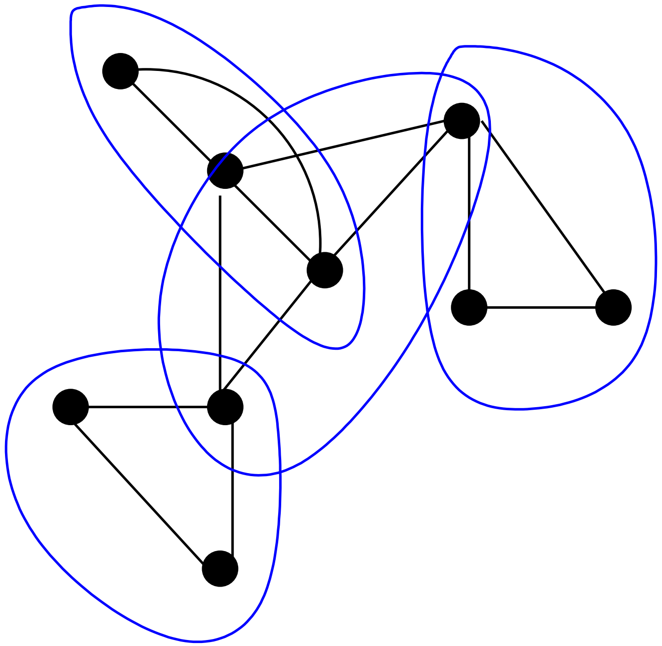
- *Spoiler* chooses a pair of pebbles a_i and b_i;
- *Duplicator* chooses a bijection $h : A \to B$ such that for pebbles a_j and $b_j (j \neq i)$, $h(a_j) = b_j$;
- *Spoiler* chooses $a \in A$ and places a_i on a and b_i on $h(a)$.

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, $\mathbb{A} \equiv^{C^k} \mathbb{B}$.

TreeWidth

The *treewidth* of a graph is a measure of how tree-like the graph is.

A graph has treewidth k if it can be covered by subgraphs of at most $k+1$ nodes in a tree-like fashion.



TreeWidth

Formal Definition:

For a graph $G = (V, E)$, a *tree decomposition* of G is a relation $D \subset V \times T$ with a tree T such that:

- for each $v \in V$, the set $\{t \mid (v, t) \in D\}$ forms a connected subtree of T; and
- for each edge $(u, v) \in E$, there is a $t \in T$ such that $(u, t), (v, t) \in D$.

The *treewidth* of G is the least k such that there is a tree T and a tree-decomposition $D \subset V \times T$ such that for each $t \in T$,

$$|\{v \in V \mid (v, t) \in D\}| \leq k + 1.$$

Cops and Robbers

A game played on an undirected graph $G = (V, E)$ between a player controlling k *cops* and another player in charge of a *robber*.

At any point, the cops are sitting on a set $X \subseteq V$ of the nodes and the robber on a node $r \in V$.

A move consists in the cop player removing some cops from $X' \subseteq X$ nodes and announcing a new position Y for them. The robber responds by moving along a path from r to some node s such that the path does not go through $X \setminus X'$.

The new position is $(X \setminus X') \cup Y$ and s. If a cop and the robber are on the same node, the robber is caught and the game ends.

Strategies and Decompositions

Theorem (Seymour and Thomas 93):
There is a winning strategy for the *cop player* with k cops on a graph G if, and only if, the tree-width of G is at most $k-1$.

It is not difficult to construct, from a tree decomposition of width k, a winning strategy for $k+1$ cops.

Somewhat more involved to show that a winning strategy yields a decomposition.

Cops, Robbers and Bijections

If G has treewidth k or more, than the *robber* has a winning strategy in the k-*cops and robbers* game played on G.

We use this to construct a winning strategy for Duplicator in the k-pebble bijection game on $\mathbf{E}_{\mathcal{G}}$ and $\tilde{\mathbf{E}}_{\mathcal{G}}$.

- A bijection $h : \mathbf{E}_{\mathcal{G}} \rightarrow \tilde{\mathbf{E}}_{\mathcal{G}}$ is *good bar* v if it is an isomorphism everywhere except at the variables $x^e a$ for edges e incident on v.
- If h is good bar v and there is a path from v to u, then there is a bijection h' that is good bar u such that h and h' differ only at vertices corresponding to the path from v to u.
- Duplicator plays bijections that are good bar v, where v is the robber position in G when the cop position is given by the currently pebbled elements.

Computational Problems from Linear Algebra

Linear Algebra is a testing ground for exploring the boundary of the expressive power of IFP $+$ C.

It may also be a possible source of new operators to extend the logic.

For a set I, and binary relation $A \subseteq I \times I$, take the matrix M over the two element field $\mathbb{Z}_2$:

$$M_{ij} = 1 \quad \Leftrightarrow \quad (i,j) \in A.$$

Most interesting properties of M are invariant under permutations of I.

Matrix Multiplication

We can write a formula $\text{prod}(x, y, A, B)$ that defines the *product* of two matrices:

$$(\exists \nu_2 < t)(t = 2 \cdot \nu_2 + 1) \quad \text{for} \quad t = \#z(A(x, z) \wedge B(z, y))$$

A simple application of **ifp** then allows us to define $\text{upower}(x, y, \nu, A)$ which gives the matrix A^ν:

$$\begin{aligned}[\mathbf{ifp}_{R,uv\mu}\ &(\mu = 0 \wedge u = v \vee \\ &(\exists \mu' < \mu)\,(\mu = \mu' + 1 \wedge \text{prod}(u, v, B/R(\mu'), A))](x, y, \nu),\end{aligned}$$

where $\text{prod}(u, v, B/R(\mu'), A)$ is obtained from $\text{prod}(u, v, A, B)$ by replacing the occurrence of $B(z, v)$ by $R(z, v, \mu')$.

Matrix Exponentiation

We can, instead, represent numbers up to $2^{|A|}$ in *binary*.

That is, a unary relation Γ interpreted over the number domain (using numbers up to $|A|$) codes the number $\sum_{\gamma \in \Gamma} 2^{\gamma}$.

Repeated squaring then allows us to define power(x, y, Γ, A) giving A^N where Γ codes a value N which may be exponential.

Non-Singularity

(Blass-Gurevich 04) show that *non-singularity* of a matrix over $\mathbb{Z}_2$ can be expressed in IFP $+$ C.

GL$(n, \mathbb{Z}_2)$—the *general linear group* of degree n over $\mathbb{Z}_2$—is the group of non-singular $n \times n$ matrices over $\mathbb{Z}_2$.

The order of GL$(n, \mathbb{Z}_2)$ divides

$$N = \prod_{i=0}^{n-1} (2^n - 2^i).$$

Thus, A is *non-singular* if, and only if, $A^N = \mathbf{I}$

Moreover, the inverse A^{-1} is given by A^{N-1}.

Summary

IFP $+$ C cannot express some *natural* problems in PTime, such as definability of equations over $\mathbb{Z}_2$.

Still, IFP $+$ C forms a natural expressivity class within PTime. It captures all of PTime on many natural classes of graphs.

Linear Algebra possibly provides a new source of extensions of IFP $+$ C.