Logics for Polynomial Time

Tutorial Part 2: Fixed Point Logics and Counting.

Anuj Dawar

University of Cambridge

JAF, Fontainebleau, 18 June 2009

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 P.

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

> A logic for P would be intermediate, in expressive power, between first-order logic and second-order logic.

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 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 *increasing* 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.

IFP

The logic IFP 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 IFP have the same expressive power **(Gurevich-Shelah 1986; Kreutzer 2004)**.

Transitive Closure

The formula

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

defines the *transitive closure* of the relation E

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

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

(Immerman; Vardi 1982)

Immerman-Vardi Theorem

$\exists <$ $\exists$State $\exists$Head $\exists$Tape

$<$ is a linear order $\wedge$

$\left.\begin{array}{l} \text{State}(t+1, s_1) \rightarrow \text{State}(t, s) \vee \ldots \\ \wedge \text{State}(t+1, s_2) \rightarrow \ldots \\ \wedge \text{Tape}(t+1, p) \leftrightarrow \text{Head}(t, p) \ldots \\ \wedge \text{Head}(t+1, h+1) \leftrightarrow \ldots \\ \wedge \text{Head}(t+1, h-1) \leftrightarrow \ldots \end{array}\right\}$ encoding transitions of M

$\wedge$at time 0 the tape contains a description of $\mathbb{A}$

$\wedge$State(max, s) for some accepting s

With a deterministic machine, the relations State, Tape and Head can be define *inductively*.

IFP 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 IFP with $<$, which is invariant under the choice of order. The set of all such sentences is not *r.e.*

IFP by itself is too weak to express all properties in P.

Evenness is not definable in IFP.

Finite Variable Logic

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

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

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.

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 anelement 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)**

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

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.

Fixed-point Logic with Counting

Immerman proposed IFP $+$ C—the extension of IFP 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*: $(\exists x < t)\, \varphi$

Counting Quantifiers

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

- 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 IFP $+$ C, there is a k such that if $\mathbb{A} \equiv^{C^k} \mathbb{B}$, then

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

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 a subset of the universe (say $X \subseteq B$)

Duplicator responds with a subset of the other structure (say $Y \subseteq A$) of the same *size*.

Spoiler then places a b_i pebble on an element of Y and *Duplicator* must place a_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 q moves, then $\mathbb{A}$ and $\mathbb{B}$ agree on all sentences of C^k of quantifier rank at most q.

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 P.

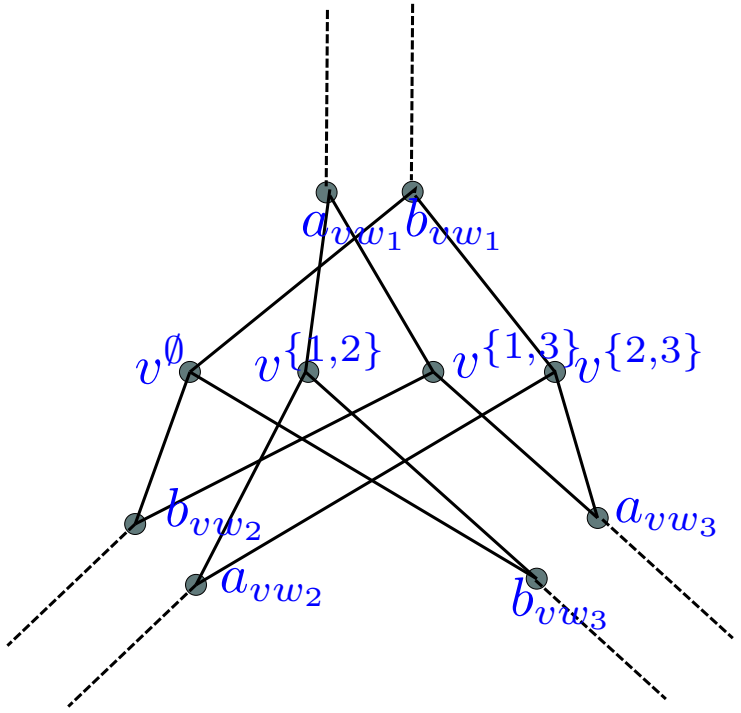
Constructing G_k and H_k

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)**.

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 $h(a)$.

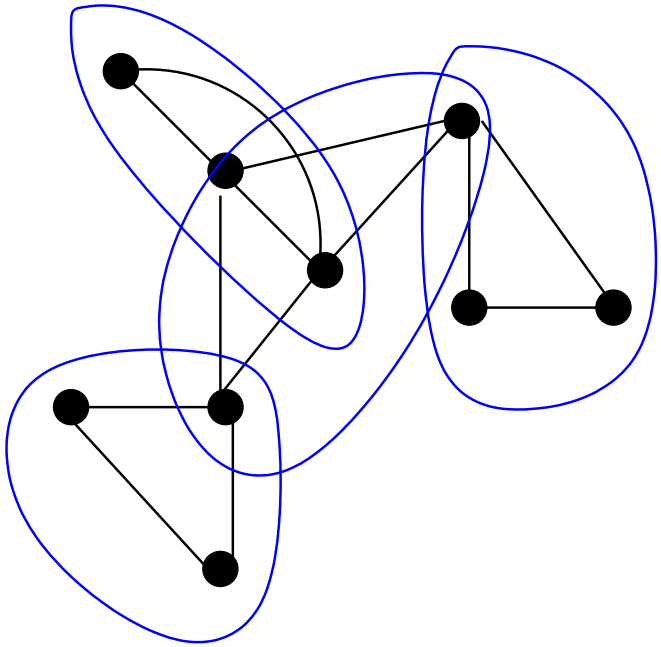
Duplicator loses if the partial map $a_i \mapsto b_i$ is not a partial isomorphism.

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 X_G and $\tilde{X}_G$.

- A bijection $h : X_G \to \tilde{X}_G$ is *good bar* v if it is an isomorphism everywhere except at the vertices v^S.
- 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.

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 P on *trees*. **(Immerman and Lander 1990)**.
2. IFP $+$ C captures P on any class of graphs of *bounded treewidth*. **(Grohe and Mariño 1999)**.
3. IFP $+$ C captures P on the class of *planar graphs*. **(Grohe 1998)**.

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.

(D., Richerby 07) shows that (2) is in some sense *optimal* in that on any class that contains *all* structures of treewidth $f(n)$ for unbounded f, it fails.