Descriptive Polynomial Time Complexity

Tutorial Part 2: Fixed Point Logics and Counting.

Anuj Dawar

University of Cambridge

Prague Fall School, 21 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 P.

A precise formulation asks for a recursive enumeration of polynomially-clocked Turing machines that are *isomorphism-invariant*.

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.

P-complete Problems

If there is any problem that is complete for P with respect to first-order reductions, then there is a logic for P.

If Q is such a problem, we form, for each k, a quantifier Q^k.

The sentence

$$Q^k(\pi_U, \pi_1, \ldots, \pi_s)$$

for a k-ary interpretation $\pi = (\pi_U, \pi_1, \ldots, \pi_s)$ is defined to be true on a structure $\mathbb{A}$ just in case

$$\pi(\mathbb{A}) \in Q.$$

The collection of such sentences is then a logic for P.

Conversely,

Theorem

If the polynomial time properties of graphs are recursively indexable, there is a problem complete for P under first-order reductions.

(D. 1995)

Proof Idea:

Given a recursive indexing $((M_i, p_i)|i \in \omega)$ of P

Encode the following problem into a class of finite structures:

$$\{(i, x)|M_i \text{ accepts } x \text{ in time bounded by } p_i(|x|)\}$$

To ensure that this problem is still in P, we need to pad the input to have length $p_i(|x|)$.

Constructing the Complete Problem

Suppose M is a machine which on input $i \in \omega$ gives a pair (M_i, p_i) as in the definition of recursive indexing. Let g a recursive bound on the running time of M.

Q is a class of structures over the signature $(V, E, \preceq, I)$.

$\mathbb{A} = (A, V, E, \preceq, I)$ is in Q if, and only if,

1. $\preceq$ is a linear pre-order on A;
2. if $a, b \in I$, $a \preceq b$ and $b \preceq a$, i.e. I picks out one equivalence class from the pre-order (say the i^{th});
3. $|A| \geq p_i(|V|)$;
4. the graph (V, E) is accepted by M_i; and
5. $g(i) \leq |A|$.

Summary

The following are equivalent:

- P is recursively indexable.
- There is a logic capturing P of the form $\mathrm{FO}(\mathbf{Q})$, where $\mathbf{Q}$ is the collection of vectorisations of a single quantifier.
- There is a complete problem in P under first-order reductions.

Another way of viewing this result is as a dichotomy.

Either there is a single problem in P such that all problems in P are easy variations of it

or, there is no reasonable classification of the problems in P.

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-dereasing* 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 $[\textbf{ifp}_{R,\mathbf{x}}\varphi](\mathbf{t})$ 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

$$\exists < \quad \exists \mathsf{State}_1 \cdots \mathsf{State}_q \exists \mathsf{Head}\ \exists \mathsf{Tape}$$

$$< \text{ is a linear order } \wedge$$

$$\left.\begin{array}{l} \mathsf{State}_1(t+1) \rightarrow \mathsf{State}_i(t) \vee \ldots \\ \wedge \mathsf{State}_2(t+1) \rightarrow \ldots \\ \wedge \mathsf{Tape}(t+1,p) \leftrightarrow \mathsf{Head}(t,p) \ldots \\ \wedge \mathsf{Head}(t+1,h+1) \leftrightarrow \ldots \\ \wedge \mathsf{Head}(t+1,h-1) \leftrightarrow \ldots \end{array}\right\} \begin{array}{l} \text{encoding} \\ \text{transitions} \\ \text{of } M \end{array}$$

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

$$\wedge \mathsf{State}(\max, s) \text{ for some accepting s}$$

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.

Recursive Indexability

Say that a formula φ of IFP in the vocabulary $\sigma \cup \{<\}$ is *order-invariant* if, for any σ-structure $\mathbb{A}$ and any two linear orders $<_1$ and $<_2$ of its universe,

$$(\mathbb{A}, <_1) \models \varphi \text{ if, and only if, } (\mathbb{A}, <_2) \models \varphi$$

Then, the following are equivalent:

- P is recursively indexable.
- There is an *r.e.* set $\mathcal{S}$ of sentences of IFP so that
  - every sentence in $\mathcal{S}$ is order-invariant; *and*
  - every order-invariant sentence of IFP has an equivalent sentence in $\mathcal{S}$.

Taking $\mathcal{S}$ to be the collection of sentences that do not mention $<$ is insufficient.

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.

P-Complete Problems

It is easily seen that IFP can express some P-complete problems such as *Alternating Transitive Closure* (ATC).

$$[\mathbf{ifp}_{R,x}(x = t \vee (D(x) \wedge \exists y(E(x,y) \wedge R(y))) \vee$$
$$(C(x) \wedge \forall y(E(x,y) \rightarrow R(y))))](s)$$

We can conclude that IFP is *not* closed under AC_0-reductions.

We can also conclude that ATC is not P-complete under FO-reductions.

It can be shown that ATC is complete for IFP under FO-reductions.

There is a P-complete problem under FO-reductions *if, and only if,* there is one under IFP-reductions.

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.

Summary

IFP $+$ C is a logic that extends first-order logic with *inflationary fixed-points* and *counting*.

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

It captures all of P on many natural classes of graphs.

There are P properties that are not in IFP $+$ C.

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