Descriptive Polynomial Time Complexity

Tutorial Part 4

Anuj Dawar
University of Cambridge

Prague Fall School, 23 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, the extension of IFP with counting is also too weak. In particular, it can not express the solvability of systems of linear equations.

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

Linear Algebra is perhaps a source of new extensions of the logic.

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.

Computational Complexity

$\oplus$L is the complexity class containing languages L for which there is a *nondeterministic, logspace* machine M such that

> $x \in L$ if, and only if, the number of accepting paths of M on input x is *odd*.

$\oplus$L contains L and is (as far as we know) incomparable with NL.

$\oplus$GAP is a natural $\oplus$L-complete problem under logspace reductions.

> $\oplus$GAP: given an *acyclic, directed* graph G with vertices s, t, is the number of distinct paths from s to t *odd*?

Computational Complexity II

The following are all $\oplus$L-complete under logspace reductions:

- Non-singularity of matrices over $\mathbb{Z}_2$;
- Inverting a matrix over $\mathbb{Z}_2$;
- Determining the rank of a matrix over $\mathbb{Z}_2$.

(Buntrock, Damm, Hertrampf, Meinel 92)

Note: $\oplus$GAP is definable in IFP $+$ C as it amounts to checking $(A_G^n)_{st}$, where A_G is the adjacency matrix of G.

IFP $+$ C over Finite Fields

Over $\mathbb{F}_q$, *matrix multiplication*; *non-singularity* of matrices; the *inverse* of a matrix; are all definable in IFP $+$ C.

determinants and more generally, the coefficients of the *characteristic polynomial* can be expressed IFP $+$ C.

(D., Grohe, Holm, Laubner, 2009)

solvability of systems of equations is *undefinable*.

the *rank* of a matrix is *undefinable*.

Rank Operators

We introduce an operator for *matrix rank* into the logic.

We have, as with $\mathrm{IFP} + \mathrm{C}$, terms of *element sort* and *numeric sort*.

We interpret $\eta(x, y)$—a *term* of numeric sort—in $\mathbb{A}$ as defining a *matrix* with rows and columns indexed by elements of A with entries $\eta[a, b]$.

$\mathrm{rk}_{x,y}\eta$ is a *term* denoting the number that is the rank of the matrix defined by $\eta(x, y)$.

To be precise, we have, for each finite field $\mathbb{F}_q$ (q prime), an operator rk^q which defines the rank of the matrix with entries $\eta[a, b] (\mathrm{mod}\, q)$.

(D., Grohe, Holm, Laubner, 2009)

IFP $+$ rk vs. IFP $+$ C

Adding rank operators to IFP, we obtain a proper extension of IFP $+$ C.

$$\#x\varphi \quad = \quad \mathsf{rk}_{x,y}[x = y \wedge \varphi(x)]$$

In IFP $+$ rk we can express the solvability of linear systems of equations, as well as the Cai-Fürer-Immerman graphs and the order on multipedes.

$\mathrm{FO} + \mathrm{rk}$

More generally, for each prime p and each arity m, we have an operator rk^p_m which binds $2m$ variables and defines the rank of the $n^m \times n^m$ matrix defined by a formula $\varphi(\mathbf{x}, \mathbf{y})$.

$\mathrm{FO} + \mathrm{rk}$, the extension of first-order logic with the rank operators is already quite powerful.

- it can express *deterministic transitive closure*;
- it can express *symmetric transitive closure*;
- it can express solvability of linear equations.

Symmetric Transitive Closure

Let $G = (V, E)$ be an *undirected graph* and let s and t be vertices in V.

Define the system of equations $\mathbf{E}_{G,s,t}$ over $\mathbb{F}_2$ with variables x_v for each $v \in V$, and equations

- for each edge $e = u, v \in E$: $\quad x_u + x_v = 0$;
- $x_s = 1 \quad x_t = 0$.

$\mathbf{E}_{G,s,t}$ is solvable if, and only if, there is no path from s to t in G.

Capturing $\mathrm{Mod}_p\mathrm{L}$

For each number p, the complexity class $\mathrm{Mod}_p\mathrm{L}$ is defined like $\oplus$L but with acceptance condition:

> $x \in L$ if, and only if, the number of accepting paths of M on input x is not $0 (\mathrm{mod}\, p)$.

For *prime* p, let FO $+$ rk^p, be the logic extending first-order logic with the rk^p operator of all arities.

> On *ordered structures*, FO $+$ rk^p captures $\mathrm{Mod}_p\mathrm{L}$.

Arity Hierarchy

In the case of $\mathsf{IFP} + \mathsf{C}$, adding counting operators of arities higher than 1 does not increase expressive power. These can all already be defined in $\mathsf{IFP} + \mathsf{C}$ with *unary* counting.

This is not the case with $\mathsf{IFP} + \mathsf{rk}$.

We prove

> For each m, there is a property definable in $\mathsf{FO} + \mathsf{rk}^2_{m+1}$ that is not definable in $\mathsf{IFP} + \mathsf{rk}_m$.

The proof is based on a construction due to Hella, and requires vocabularies of increasing arity.

It is conceivable that *over graphs*, the arity hierarchy collapses.

Games for Logics with Rank

Define the equivalence relation $\mathbb{A} \equiv^{R^k_{p,m}} \mathbb{B}$ to mean that $\mathbb{A}$ and $\mathbb{B}$ are not distinguished by any formula of $\mathsf{FO} + \mathsf{rk}$ using operators rk^p_m and with at most k variables.

This equivalence relation has a characterisation in terms of *games*.

(**Holm 2009**)

This game can been used to show that for *distinct* primes p, q, solvability of linear equations $\mathrm{mod}\ q$ cannot be defined in IFP with operators rk^p_1.

Games for Logics with Rank

The game is played with k pairs of pebbles. At each move

- *Spoiler* picks $2m$ pebbles from $\mathbb{A}$ and the corresponding pebbles from $\mathbb{B}$.
- *Duplicator* reponds with
  - a partition $\mathbf{P}$ of $A^m \times A^m$
  - a partition $\mathbf{Q}$ of $B^m \times B^m$
  - a bijection $f : \mathbf{P} \to \mathbf{Q}$ such that for all labellings $\gamma : \mathbf{P} \to \mathbb{Z}_p$

$$\text{rank}(M_{\gamma}^{\mathbf{P}}) = \text{rank}(M_{\gamma \circ f^{-1}}^{\mathbf{Q}})$$

- *Spoiler* chooses a part $P \in \mathbf{P}$ and places the chosen pebbles on a tuple in P and the matching pebbles on a tuple in $f(P)$.

Approximations of Isomorphism

For each k, the relation $\equiv^{C^k}$ is decidable in *polynomial time*.

It provides an approximation of *graph isomorphism*.

This is also known as the *Weisfeiler-Lehmann* method.

The *CFI* construction shows that there is no k for which $\equiv^{C^k}$ coincides with graph isomorphism.

Approximations of Isomorphism

Grohe's capturing result on proper minor-closed classes of graphs shows the following.

> For any *proper minor-closed class* C of graphs, there is a k such that $\equiv^{C^k}$ coincides with isomorphism on C.

What can we say about the equivalence relation $\equiv^{R^k}$?

Equations over Groups and Rings

We can define systems of equations, not just over *fields* but over *finite rings* or *groups*.

For rings and *Abelian* groups, the problems are solvable in polynomial time.

There is corresponding notion of *rank*, and it is not clear that these problems can be expressed in $\mathrm{IFP} + \mathrm{rk}$.

We can show that the solvability problems for rings, fields and Abelian groups can be reduced (in $\mathrm{IFP} + \mathrm{C}$) to that for *finite, commutative, local rings*.

(D, Holm, Kopczynski, Pakusa 2011)

Choiceless Polynomial Time

Choiceless Polynomial Time ($\tilde{C}PT$) is a class of computational problems defined by **Blass, Gurevich and Shelah**.

It is based on a *machine model (Gurevich Abstract State Machines)* that works directly on a relational structure (rather than on a string representation).

The machine can access the collection of hereditarily finite sets over the universe of the structure.

$\tilde{C}PT$ is the polynomial time and space restriction of the machines.

$\tilde{C}PT$ is strictly more expressive than IFP, but still cannot express counting properties.

Consider $\tilde{C}PT(\mathrm{Card})$—the extension of $\tilde{C}PT$ with counting.

Does it express all properties in PTime?

Choiceless Polynomial Time

$\tilde{\mathsf{C}}\mathsf{PT}$ can express the property of **Cai, Fürer and Immerman**.

Any program of $\tilde{\mathsf{C}}\mathsf{PT}(\mathsf{Card})$ that expresses the CFI property must use sets of *unbounded rank*.

$\mathrm{IFP} + \mathrm{C}$ can be translated to programs of $\tilde{\mathsf{C}}\mathsf{PT}(\mathsf{Card})$ of bounded rank.

(D., Richerby and Rossman 2008)

Research Directions

- Is the equivalence relation $\equiv^{R^k}$ decidable in polynomial time? Is it definable in IFP $+$ rk? Could there be a fixed k for which it is the same as isomorphism?
- Is solvability of systems of linear equations over finite rings in IFP $+$ rk?
- Are there any problems in PTime that are not definable in IFP $+$ rk?
- Show for some problem definable in IFP $+$ rk that it is not definable in FO $+$ rk.
- Show for any concrete problem (say an NP-complete one) that it is not definable in IFP $+$ rk.

Research Directions II

- Could IFP $+$ rk be sufficient to capture PTime on bounded-degree graphs?
- How does the expressive power of IFP $+$ rk compare with $\tilde{\mathsf{C}}\mathsf{PT}(\mathsf{Card})$?
- Is matrix rank definable in $\tilde{\mathsf{C}}\mathsf{PT}(\mathsf{Card})$?